



INTELLIGENCE OMBUDSPERSONS' OFFICE
OF THE REPUBLIC OF LITHUANIA

ANNUAL ASSESSMENT OF THE LAWFULNESS OF THE ACTIVITIES OF INTELLIGENCE INSTITUTIONS AND THEIR COMPLIANCE WITH REQUIREMENTS FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

2025

ANNUAL ASSESSMENT OF THE LAWFULNESS OF THE ACTIVITIES OF INTELLIGENCE INSTITUTIONS AND THEIR COMPLIANCE WITH REQUIREMENTS FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS 2025

Opening Remarks	03
Summary	04
I. Key Directions of Intelligence Oversight Activities in 2025	06
II. Inspections Conducted by the Intelligence Ombudsperson	08
1. Compliance of the Authorisation of Intelligence Measures with the Principle of Legality and the Requirements for the Protection of Human Rights and Fundamental Freedoms	
2. Implementation of Recommendations Following the 2024 Inspection on the Effectiveness of the Organisation of Internal Control within Intelligence Institutions	
3. Inspection of the Compliance of Internal Security Arrangements within AOTD with Applicable Laws and Other Legal Acts, and the Requirements for the Protection of Human Rights and Fundamental Freedoms	
4. Planned Inspections of the Legality of the Activities of Intelligence Institutions in 2026	
III. Legal Regulation of Intelligence Activities	11
1. Draft Amendments to the Law on Intelligence Ombudspersons and Related Legislative Proposals	
2. Amendments to the Law on Intelligence of the Republic of Lithuania	
3. Draft Amendments to the Law on the Use of the Polygraph of the Republic of Lithuania	
IV. Complaints	14
1. Complaints Related to the Protection of the Rights of Foreign Nationals	
2. Complaints Related to Criminal Intelligence	
V. Technological Challenges to Privacy and Personal Data Protection: Implications for the Oversight of Intelligence Institutions	16
VI. Challenges	18

TO THE SEIMAS OF THE REPUBLIC OF LITHUANIA,

Pursuant to Article 30 of the Law on Intelligence Ombudspersons of the Republic of Lithuania, I hereby submit to the Seimas of the Republic of Lithuania the Annual Assessment of the Lawfulness of the Activities of Intelligence Institutions and their Compliance with Requirements for the Protection of Human Rights and Fundamental Freedoms, as well as the 2025 Activity Report.

This is the third annual report reviewing the legality of the activities of the intelligence institutions of the Republic of Lithuania and their compliance with the requirements for the protection of human rights and fundamental freedoms, as well as the third activity report on the independent external expert oversight of these institutions carried out since its establishment in 2023.

This report and activity review present the key results of intelligence oversight in 2025, offer insights into identified systemic challenges, and set out proposals for improving the legal framework governing intelligence and its oversight. Particular attention is devoted to preventive activities, the importance of training and consultations, the development of international cooperation, and the strengthening of the effectiveness of the oversight system.

It is hoped that the insights and recommendations provided in this report will contribute to informed decision-making by the Seimas of the Republic of Lithuania, promote the consistent development of legislation in the field of intelligence oversight, and create the conditions for further strengthening the legality of intelligence activities and the protection of human rights and fundamental freedoms in a democratic state.



Head of the Intelligence Ombudspersons' Office,
Intelligence Ombudsperson

DR. NORTAUTAS STATKUS

A handwritten signature in blue ink, appearing to read 'N. Statkus'.

SUMMARY

**INSPECTIONS OF THE ACTIVITIES
OF INTELLIGENCE INSTITUTIONS**

In 2025, three inspections were conducted:

- An inspection of the compliance of the authorisation of intelligence information collection measures with the principle of legality governing the activities of intelligence institutions, as well as with the requirements for the protection of human rights and fundamental freedoms. The inspection of the Second Investigation Department under the Ministry of National Defence (hereinafter – AOTD) has been completed, with no irregularities identified, while the deadline for completing the inspection of the State Security Department (hereinafter – VSD) has been extended until the end of 2026.
- A follow-up inspection (implementation of recommendations) of the effectiveness of the organisation of internal control within intelligence institutions, based on the inspection conducted in 2024. It was established that the intelligence institutions had implemented the recommendations provided.
- An ad hoc inspection concerning the compliance of AOTD internal security arrangements with applicable laws and other legal acts and with the requirements for the protection of human rights and fundamental freedoms. This inspection is ongoing and is planned to be completed in 2026.

**EXAMINATION OF INDIVIDUAL
COMPLAINTS AND INVESTIGATIONS**

In 2025, a total of 15 complaints were received:

- 2 complaints were not examined, as they did not meet the requirements established by the Law on Intelligence Ombudspersons of the Republic of Lithuania;
 - 5 complaints were not examined, as they fell outside the competence of the Intelligence Ombudsperson (of these, 3 were related to criminal intelligence);
 - In relation to 5 complaints, 4 investigations were initiated (two complaints were consolidated into a single investigation):
 - 2 complaints concerning the same subject matter (related to the lawfulness of personal data processing and the assessment of a threat to national security) were merged into one investigation, which was subsequently discontinued due to the initiation of judicial proceedings;
 - 1 complaint concerning a violation of time limits under the Law on the Legal Status of Foreigners of the Republic of Lithuania was examined; the investigation was terminated after the applicant withdrew the complaint;
 - 1 complaint concerning the lawfulness of personal data processing was examined and dismissed as unfounded;
 - 1 complaint concerning the lawfulness and justification of the processing of personal data and other information about an individual was examined and dismissed as unfounded;
- 2 complaints were refused for examination, because they had already been examined or brought before the court;
- 1 complaint was withdrawn after the issue was resolved through the mediation of the Intelligence Ombudsperson.

IMPROVEMENT OF THE LEGAL FRAMEWORK

- The Office prepared and submitted to the Seimas of the Republic of Lithuania proposals for amendments to legal acts regulating the activities of intelligence institutions and their oversight. The Seimas endorsed the draft legislation (the draft Law on Intelligence Ombudspersons, the draft Law on Intelligence, and the draft Law on Criminal Intelligence) after presentation and resolved to consider these drafts during the Spring Session of 2026 in the Committee on National Security and Defence, the Committee on Human Rights, and the Committee on Legal Affairs. The adoption of the proposed amendments would reinforce the institutional foundations of the Office of the Intelligence Ombudspersons and ensure the conditions necessary for it to function effectively as an independent authority for the protection of human rights.

INTERNATIONAL COOPERATION

- International cooperation remains an important area of activity for the Office of the Intelligence Ombudspersons, enabling the exchange of best practices with foreign counterparts and contributing to the development of transparent, effective, and professional oversight of intelligence institutions.

In 2025, representatives of the Office participated in workshops organised by the Council of Europe, the Conference of European Intelligence Oversight Bodies, and consultations with representatives of the Verkhovna Rada of Ukraine. In addition, bilateral meetings and exchanges of experience were held with oversight institutions from Finland, Canada, Ukraine, and other countries.

INSPECTION PRIORITIES FOR 2026

Two inspections are planned:

- To assess whether intelligence institutions, in carrying out intelligence and counterintelligence tasks, use intelligence information and process personal data lawfully, in compliance with the Law on Intelligence, as well as human rights and personal data protection requirements.
- A follow-up inspection to evaluate how intelligence institutions have implemented the recommendations issued during the 2024–2025 inspection concerning the compliance of intelligence information provided to national security authorities with the principles of timeliness, objectivity, and clarity governing the activities of intelligence institutions.

I. KEY DIRECTIONS OF INTELLIGENCE OVERSIGHT ACTIVITIES IN 2025

Oversight of intelligence activities represents one of the most complex challenges in democratic governance. A democratic state must reconcile the imperatives of national security with the protection of human rights and fundamental freedoms. Intelligence institutions are entrusted with extensive powers, including the use of covert intelligence methods, the monitoring of processes posing threats to national security, the provision of assessments relevant to national security policy decisions, and the mitigation of threats and risk factors to national security. These powers are essential in responding to contemporary threats—such as espionage, sabotage, deliberate damage to critical infrastructure, unlawful influence by foreign states, including interference in elections and other domestic processes, terrorism, cyber incidents, and hybrid attacks. However, their use must be clearly defined by law and subject to continuous oversight in order to prevent abuse and to maintain public trust in intelligence institutions.

The nature of intelligence activities characterised by secrecy, speed, and discretion inevitably alters the balance between state power and individual rights. Individuals are often unaware that intelligence measures are being applied to them and therefore lack a genuine opportunity to challenge such measures, creating structural gaps in accountability and the protection of individual rights. For this reason, democratic states entrench the principle of the rule of law to ensure that security and freedom are not mutually exclusive objectives; rather, they must be reconciled through the rule of law, institutional checks and balances, and consistent, continuous, and professional oversight.

In Lithuania, a multi-layered system of intelligence oversight is in place to ensure both the effectiveness and the lawfulness of intelligence activities. This system includes parliamentary oversight (notably through the Seimas Committee on National Security and Defence), prior judicial authorisation in cases involving intelligence-gathering measures that significantly interfere with private life, executive oversight and coordination, and internal control within intelligence institutions. Financial oversight mechanisms also contribute to the overall framework of accountability, while issues relating to the lawfulness of personal data processing require a particularly clear delineation of institutional competences, taking into account the specific nature of national security and defence objectives.

While internal institutional self-control is often regarded as one of the most effective forms of oversight, it does not in itself ensure effective protection of human rights, particularly in light of the secrecy and limited transparency inherent in intelligence activities. Consequently, independent external oversight of intelligence institutions assumes particular importance.

In this context, the Seimas of the Republic of Lithuania established the institution of Intelligence Ombudspersons with the aim of strengthening the effective protection of human rights. The Intelligence Ombudspersons carry out continuous, independent, and professional oversight of the lawfulness of the activities of intelligence institutions. They are granted access to classified information and assess not only the formal compliance of decisions and actions of intelligence institutions and officers with legal requirements, but also the extent to which standards for the protection of human rights and freedoms are upheld. The purpose of this oversight is not merely to disclose information about potential violations or to promote transparency as an end in itself, but to ensure, through an independent external institutional control mechanism, that the exercise of covert state powers complies with the Constitution and respects human rights and freedoms.

Having commenced its activities in 2023, the Office of the Intelligence Ombudspersons (hereinafter – the Office) has been developing a system of continuous external expert oversight, based on systematic inspections, consultations, the issuance of recommendations, and dialogue with intelligence institutions and other public authorities.

In response to the evolving security environment, technological developments, and increasing international commitments, the priorities of intelligence oversight in 2025 were further oriented towards strengthening the institutional capacity of the Office. Particular attention was devoted to training, consultations, and methodological assistance for officers of intelligence institutions, with the aim of preventing potential violations of the law and ensuring that intelligence activities are consistently carried out in accordance with the principles of legality, proportionality, and necessity. At the same time, systematic oversight of these activities was continued, including the monitoring of the implementation of recommendations and the refinement of methodologies in areas where risks to human rights are most significant.

International cooperation remained an integral area of activity. As intelligence activities and their oversight increasingly transcend national borders, the exchange of experience with oversight bodies of NATO and European Union Member States, as well as participation in international networks and discussions, has become an essential source for improving the national oversight model and adopting best practices.

The improvement of the legal framework also constituted an important area of focus. Practical experience in the oversight of intelligence activities has revealed regulatory gaps, as well as potential conflicts

and overlaps between legal norms, necessitating consistent proposals for legislative amendments. The Office of the Intelligence Ombudspersons submitted a range of proposals for amendments to laws and other legal acts. Through such legislative initiatives and the provision of expert opinions, the aim was to strengthen the prevention of legal violations, enhance the effectiveness of oversight, and ensure a higher standard of protection of human rights and freedoms in the field of intelligence activities.

These directions of activity are reflected in the Strategic Action Plan of the Office of the Intelligence Ombudspersons for 2026–2028 and provide the foundation for continued independent, effective, and professional oversight of intelligence institutions, strengthening both national security and public trust in the state and its institutions.



II. INSPECTIONS CONDUCTED BY THE INTELLIGENCE OMBUDSPERSON

Oversight of the activities of intelligence institutions is carried out through inspections and the examination of complaints (reports). Inspections constitute the principal form of supervisory activity of the Intelligence Ombudsperson of the Republic of Lithuania (hereinafter – the Intelligence Ombudsperson). Article 11 (1) of the Law on Intelligence Ombudspersons of the Republic of Lithuania (hereinafter – the Law) establishes the duty of the Intelligence Ombudsperson to conduct continuous oversight of the legality of the activities of intelligence institutions, encompassing both the actions of intelligence institutions and intelligence officers, as well as the decisions adopted by them.

The Intelligence Ombudsperson exercises oversight by conducting planned, unscheduled (ad hoc), and follow-up (implementation review) inspections, initiating investigations where there are grounds to do so, and examining complaints and reports. Inspections assess whether the activities of intelligence institutions, the actions of intelligence officers, and the decisions they adopt comply with laws and other legal acts, the requirements for the protection of human rights and fundamental freedoms, and the principles of legality, reasonableness and proportionality.

During inspections, the Intelligence Ombudsperson carries out monitoring of the activities of intelligence institutions – namely, a systematic, theme-based assessment of the activities of intelligence institutions and the decisions taken by intelligence officers, with a view to determining their legality, reasonableness, proportionality, and compliance with the requirements for the protection of human rights and fundamental freedoms. The findings of inspections are based on the analysis of information, data, and documents collected during the inspections and form the basis for deciding whether there are grounds to initiate an investigation.

1. Compliance of the Authorisation of Intelligence Measures with the Principle of Legality and the Requirements for the Protection of Human Rights and Fundamental Freedoms

By decision of 16 April 2025, the Intelligence Ombudsperson initiated an inspection of the compliance of the authorisation of intelligence information collection measures carried out in 2022–2024 by the Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania with the principle of legality governing the activities of intelligence institutions, as well as with the requirements for the protection of human rights and fundamental freedoms (hereinafter – the Inspection of the Authorisation of Measures).

During the inspection, an assessment was conducted as to whether the internal legal acts, processes, and procedures of the intelligence institutions

governing the authorisation and extension of intelligence information collection measures were in compliance with the requirements of the Law on Intelligence of the Republic of Lithuania (hereinafter – the Law on Intelligence). In addition, the legal and factual grounds underlying decisions to apply to a court for authorisation to carry out sanctioned measures were analysed, as well as how compliance of such applications with Article 13(3) of the Law on Intelligence, and with the principles of legality, reasonableness, proportionality, and the protection of human rights and fundamental freedoms, was ensured within the intelligence institutions.

The inspection also examined the practices of intelligence institutions in processing personal data for the purposes of national security or defence in the context of authorised measures. In this regard, the assessment covered compliance with the requirements of lawful personal data processing, the internal control mechanisms applied within institutions, and the implementation of requirements related to the storage of data collected through authorised measures, including the retention periods and procedures applicable to special categories of personal data.

The assessment of the compliance of authorised intelligence information collection measures with the principles of legality and the requirements for the protection of human rights and fundamental freedoms extended beyond a formal review of adherence to legal provisions, encompassing also the reasonableness of decision-making and the proportionality of the measures applied.

The assessment initially examined whether the institutions acted within the scope of their legally conferred powers, adhered to established internal procedures, and based their decisions on applicable legal provisions. However, formal compliance with legal requirements alone was not deemed sufficient. Accordingly, a further, substantive assessment was undertaken to determine whether decisions were based on all relevant factual circumstances, whether they were consistent and impartial, and whether the conclusions drawn reasonably followed from the established facts.

Moreover, an assessment was carried out as to whether the measures applied were suitable for achieving the intended objectives and whether they were not excessive. In this context, particular attention was paid to whether the same objectives could have been attained by means less restrictive of individual rights, as well as to whether the benefits achieved were proportionate to the limitations imposed on individual rights or legitimate interests. This assessment sought to ascertain that the activities of intelligence institutions are not only lawful, but also well-founded, proportionate, and consistent with the requirements for the protection of fundamental human rights.

The inspection established that the assessment of activities related to the authorisation of intelligence information collection measures required differing time resources across intelligence institutions. During the period 2022–2024, the State Security Department (VSD) applied to the courts for authorisation to carry out sanctioned measures significantly more frequently than the Second Investigation Department (AOTD). Consequently, the evaluation of this aspect of VSD's activities required greater time resources on the part of the Intelligence Ombudsperson, as well as institutional resources from VSD.

By official communication, VSD informed the Intelligence Ombudsperson that the preparation and submission of the requested information would require additional significant time resources and provided a preliminary schedule for 2025–2026 for the review and assessment of the information necessary for the inspection. In light of these circumstances, the Intelligence Ombudsperson decided to extend the deadline for the inspection of the authorisation of intelligence information collection measures carried out by VSD in 2022–2024 until 31 December 2026.

The inspection of AOTD has been completed. It was established that the authorisation of intelligence information collection measures within AOTD complies with the principles of legality, respect for human rights and fundamental freedoms, and the requirements governing the processing of personal data.

2. Implementation of Recommendations Following the 2024 Inspection on the Effectiveness of the Organisation of Internal Control within Intelligence Institutions

The follow-up inspection was aimed at assessing how the intelligence institutions implemented the recommendations issued by the Intelligence Ombudsperson following the 2024 inspection on the effectiveness of the organisation of internal control. This inspection established that both AOTD and VSD had fully implemented all recommendations provided by the Intelligence Ombudsperson.

This inspection was combined with an ad hoc inspection initiated by the Intelligence Ombudsperson on 2 July 2025 concerning circumstances described in complaints submitted by AOTD intelligence officers, relating to the conduct of the Director of AOTD, Colonel E. Paulavičius, and their potential relevance to the competence of the Intelligence Ombudsperson, with a view to determining whether there were grounds to initiate an investigation.

As the Ministry of National Defence and AOTD did not provide the information requested by the Intelligence Ombudsperson and necessary for this inspection — namely, copies of the complaints submitted by AOTD intelligence officers, a copy of the findings of the fact-finding inquiry conducted by the General Inspectorate of the Ministry of National Defence, and other material related to the circumstances described in those complaints — the Intelligence Ombudsperson decided on 26 August 2025 to merge this ad hoc

inspection with the ongoing follow-up inspection concerning the implementation of recommendations issued following the 2024 inspection on the effectiveness of the organisation of internal control within AOTD. However, even during that inspection, it was not possible to assess whether the circumstances described in the complaints submitted by AOTD intelligence officers fell within the competence of the Intelligence Ombudsperson or whether there were grounds to initiate an investigation, because the data necessary for conducting the inspection had not been received.

The Intelligence Ombudsperson decided that the compliance of AOTD internal legal acts governing the prevention of psychological harassment (mobbing) with laws and other legal requirements, as well as the application of psychological harassment prevention measures within AOTD, would be assessed as part of an ad hoc inspection of the compliance of AOTD internal security arrangements with laws, other legal acts, and the requirements for the protection of human rights and fundamental freedoms.

3. Inspection of the Compliance of Internal Security Arrangements within AOTD with Applicable Laws and Other Legal Acts, and the Requirements for the Protection of Human Rights and Fundamental Freedoms

In July 2025, an ad hoc inspection was initiated concerning the compliance of internal security arrangements within AOTD with applicable laws and other legal acts and with the requirements for the protection of human rights and fundamental freedoms. The purpose of the inspection is to assess whether there are grounds to initiate an investigation by the Intelligence Ombudsperson.

During the inspection, AOTD's internal legal acts governing internal security were analysed, with particular attention given to both their content and their practical application. In addition, the relevant AOTD units and individual intelligence officers responsible for ensuring internal security were identified, and their functions and scope of responsibility were assessed.

The inspection further examines the measures and actions aimed at preventing and mitigating both external and internal factors that may pose risks to the security of AOTD's activities, infrastructure, information, and personnel.

Within the scope of the inspection, particular attention is also given to how professional training and capacity-building were organised in 2024–2025 for the AOTD internal security unit, other relevant AOTD units, and individual intelligence officers responsible for internal security. This includes an assessment of professional development methods, training topics, their frequency and number, as well as the practice of instructing AOTD personnel on internal security matters.

The inspection is ongoing and is expected to be completed in 2026.

4. Planned Inspections of the Legality of the Activities of Intelligence Institutions in 2026

In 2026, it is planned to continue inspections of the legality of the activities of intelligence institutions that were initiated previously. The inspection of the compliance of the authorisation of intelligence measures carried out by the VSD with the principle of legality governing the activities of intelligence institutions, as well as with the requirements for the protection of human rights and fundamental freedoms, will be further pursued. The inspection concerning the compliance of internal security arrangements within AOTD with applicable laws and other legal acts and with the requirements for the protection of human rights and fundamental freedoms, will also be continued.

In addition to the ongoing inspections, new inspections of the legality of the activities of intelligence institutions are planned for 2026.

The first inspection will examine whether the use of collected intelligence information and the processing of personal data in the implementation

of intelligence and counterintelligence tasks comply with the principle of legality governing the activities of intelligence institutions as established in the Law on Intelligence, as well as with the requirements for the protection of human rights and fundamental freedoms and for personal data protection. This inspection will analyse how the principle of legality is observed within institutions when intelligence information is used and personal data are processed, and will assess whether these activities comply with standards for the protection of human rights and fundamental freedoms.

An implementation review will also be carried out to assess how intelligence institutions have implemented the recommendations issued following the 2024–2025 inspection on the compliance of intelligence information provided to national security institutions with the principles of timeliness, objectivity, and clarity governing the activities of intelligence institutions. This review will analyse the measures taken to implement the recommendations and their actual impact on the practice of providing intelligence information.



III. LEGAL REGULATION OF INTELLIGENCE ACTIVITIES

1. Draft Amendments to the Law on Intelligence Ombudspersons and Related Legislative Proposals

Effective oversight of the activities of intelligence institutions is one of the fundamental principles of a democratic state. In order to ensure a clear, coherent, and consistent legal framework governing intelligence activities and their oversight, proposals were prepared and submitted to refine the existing legislation.

On 13 May 2025, the Seimas registered the draft Law on Intelligence Ombudspersons and accompanying draft laws (Nos. XVP-422–XVP-424), including the draft Law on Intelligence Ombudspersons, the draft Law on Intelligence, and the draft Law on Criminal Intelligence¹. On 17 December 2025, the Seimas approved these legislative proposals for consideration and decided to examine them during the 2026 spring session of the Seimas in the Committee on National Security and Defence, the Committee on Human Rights, and the Committee on Legal Affairs.

The proposed amendments aim to clarify the functions and powers of the Intelligence Ombudsperson and the staff of the Office, which are necessary for the continuous oversight of the legality of the activities of intelligence institutions. It is proposed to refine the scope of access to intelligence and criminal intelligence information, including documents and data, as well as information, documents, and data processed within the information systems of intelligence institutions. The amendments also seek to more clearly define the right of the Intelligence Ombudsperson to obtain decisions of intelligence institutions concerning the initiation of intelligence information collection measures in the course of carrying out intelligence tasks, as well as consolidated information from courts regarding their rulings on the authorisation of such measures.

The amendments establish the right of the Intelligence Ombudsperson to assess not only the legality of the activities of intelligence institutions, but also their reasonableness and proportionality, taking into account that intelligence activities may involve restrictions on individual rights and freedoms, the assessment of which must comply with the principles of legality, reasonableness and proportionality. Furthermore, the amendments seek to ensure legal coherence by clearly defining the role of the Intelligence Ombudsperson in the independent external oversight of criminal intelligence activities, as well as by creating the conditions for courts examining matters related to intelligence activities to seek, where appropriate, an

expert opinion from the Intelligence Ombudsperson. They also aim to eliminate potential ambiguities in the legal framework concerning the provision of information to institutions responsible for the oversight of intelligence activities, thereby ensuring consistent and coherent application of the law in practice.

The implementation of the proposed legislative amendments would strengthen the institutional capacity of the Office and create the conditions for it to function as an effective human rights institution—capable of carrying out independent assessments of the activities of intelligence institutions and providing reliable assurance to both the Seimas of the Republic of Lithuania and the public that human rights and fundamental freedoms are respected in intelligence activities and that personal data are processed in compliance with legal requirements.

2. Amendments to the Law on Intelligence of the Republic of Lithuania

In response to the evolving geopolitical and security environment, the increasing complexity of external threats, and the need to ensure a prompt and effective response to risks to national security, amendments to the Law on Intelligence were initiated². These amendments were adopted on 23 December 2025. They significantly expand the scope of the activities of intelligence institutions by introducing a revised definition of intelligence, establishing an additional method of intelligence information collection—namely, intelligence tasking—and extending the powers of intelligence institutions to apply measures that restrict individual rights. These changes have a direct impact on the protection of the right to private life, personal data protection, the inviolability of the home, and other fundamental rights, and therefore their assessment from a human rights perspective remains of particular importance.

One of the key amendments introduces the possibility, in exceptional circumstances, to apply court-authorised intelligence information collection measures without prior judicial authorisation, where this is necessary for the implementation of intelligence and counterintelligence tasks and for taking urgent action to avert threats and risks to the national security and interests of the Republic of Lithuania. In such cases, the decision is taken by the head of the intelligence institution or an authorised official, with an obligation to apply to a court within 24 hours for subsequent

1 Draft Law Amending Articles 2, 3, 4, 5, 11, 12, 19, 25 and 26 of the Law on Intelligence Ombudspersons No. XIV-868. Available online: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/216597002fd911f09cbcab0ff4d74843?jfwid=-j99h4nnqi>

2 Draft Law Amending Articles 2, 5, 7, 9, 11, 13, 14, 18, 19, 24, 29, 33, 40, 43, 45, 49, 50, 55, 57, 60, 64, 64-1, 69, 70 and 71 of the Law on Intelligence of the Republic of Lithuania No. VIII-1861 and Supplementing the Law with Annex 3. Available online: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/02f44b60d75211f0948bfb5fa1e0c51b?jfwid=-137aoq8qto>

judicial approval of the lawfulness and reasonableness of the measures. Although the law provides for ex post judicial oversight and the obligation to destroy data where authorisation is not granted, this regulatory model implies that the lawfulness and reasonableness of measures restricting individual rights are assessed only after such measures have already been carried out.

Additional human rights sensitivities arise from the provisions allowing the covert collection of biometric and other particularly sensitive personal data (such as fingerprints, voice samples, and odour samples), as well as the use of various marking techniques for the identification of objects. These measures entail a deeper interference with private life and personal data protection and, under international human rights standards, require clear legal regulation, the safeguarding of proportionality in the application of intelligence measures, and effective independent oversight.

In the assessment of the Office of the Intelligence Ombudsperson, the proposed amendments to the Law on Intelligence expand the discretion and operational scope of intelligence institutions, thereby increasing the importance of independent oversight in ensuring that intelligence activities are conducted in compliance with the requirements for the protection of human rights and fundamental freedoms. At present, taking into account the application practice of existing legal provisions and differences in their interpretation, the scope of the Office's oversight powers does not in all cases allow for comprehensive and effective monitoring of compliance with human rights standards.

It should be noted that draft amendments to the Law on Intelligence Ombudspersons and related legislation have been registered in the Seimas and approved at the submission stage, and are scheduled for consideration during the upcoming spring session. It is expected that the adoption of these legislative amendments will contribute to strengthening independent oversight mechanisms and ensure that the expanded powers of intelligence institutions are balanced by adequate and effective control measures in line with the Constitution of the Republic of Lithuania and the standards of the European Convention on Human Rights.

The amendments to the Law on Intelligence entered into force on 1 February 2026. The Intelligence Ombudsperson will assess the internal legal acts (or their amendments) of intelligence institutions adopted for the implementation of these legislative changes, particularly those related to the conduct of intelligence and counterintelligence activities.

It will also be assessed whether, following the entry into force of the amendments, intelligence information collection measures provided for in Article 13(3) of the Law on Intelligence were applied in exceptional cases during the first quarter of 2026 in accordance with the procedure established therein. In reviewing the implementation of such court-authorised measures, particular attention will be paid to the grounds on which these urgent actions were undertaken in exceptional circumstances, as well as to other supporting information.

3. Draft Amendments to the Law on the Use of the Polygraph of the Republic of Lithuania

When assessing the amendments to the Law on Intelligence in the context of human rights protection and independent oversight, it is also important to consider other legislative initiatives that may affect the exercise of individual rights in the field of national security. Alongside the amendments to the Law on Intelligence, which expand the powers of intelligence institutions and introduce new instruments for the conduct of intelligence activities, the Seimas is also considering draft amendments to the Law on the Use of the Polygraph of the Republic of Lithuania³ (hereinafter – the Law on the Use of the Polygraph). The provisions of this draft are closely related to mechanisms for assessing the reliability of individuals and ensuring national security.

An assessment of the draft amendments to the Law on the Use of the Polygraph indicates that the proposed changes would alter the conditions for the use of the polygraph and the procedures for decision-making in the context of reliability screening. These changes may have implications for the protection of human rights and the principle of legal certainty.

The draft proposes to revise the procedure for initiating polygraph examinations by removing the requirement for a request from the head of the institution in which the individual serves or is employed. It should be noted that, while such a decision-making model is intended to strengthen protection against possible discrimination, it also highlights the need for additional safeguards to ensure that decisions are well-founded and transparent. In the view of the Office of the Intelligence Ombudspersons, it is particularly important to provide for the possibility of an additional independent review in cases where doubts arise as to whether a negative polygraph examination finding is well-founded.

3 Draft Law Amending Articles 2, 4, 5, 7, 8, 9 and 10 of the Law on the Use of the Polygraph No. VIII-1906. Available online: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/1bdedd404a8d11f0a19dcea0bcc863ad?positionInSearchResults=1&searchModelUUID=06a1f350-4332-4442-bd54-0bd232b217f7>

It should also be noted that the current legal framework continues to leave uncertainties regarding the legal consequences for an individual who refuses to undergo a polygraph examination, particularly in cases involving the revocation of an existing authorisation to work with or access classified information. In this respect, the relationship between the provisions of the Law on the Use of the Polygraph and the Law on State and Official Secrets is not sufficiently clear, which may raise concerns regarding legal certainty and the protection of legitimate expectations.

In light of the above, in order to ensure a coherent and clear legal framework, it would be appropriate to harmonise the provisions of the Law on the Use of the Polygraph with those of the Law on State and Official Secrets of the Republic of Lithuania, by clearly defining both the conditions for the use of the polygraph and the grounds for granting or revoking authorisations to work with or access classified information. Such alignment of legal provisions would contribute to well-founded decision-making and to ensuring proportionate and effective legal protection of individual rights in the field of national security.



IV. COMPLAINTS

The analysis of complaints examined in 2025 demonstrates that the role of the Office of the Intelligence Ombudsperson in ensuring the legality of the activities of intelligence institutions and the protection of human rights remains significant and continues to strengthen consistently. The increasing number of complaints received is attributable not so much to potential shortcomings in the activities of intelligence institutions, but rather to growing public awareness of the possibility to submit complaints and increasing trust in external, independent oversight.

An analysis of the substance of the complaints indicates that a substantial proportion of them concern the lawfulness of the processing of personal data and the substantiation of decisions related to potential threats to national security. This reflects the continuing need to balance the interests of national security with the protection of the rights of natural and legal persons. In such situations, effective oversight requires not merely formal review, but thorough and substantive scrutiny, which is ensured through inspections and investigations conducted by the Intelligence Ombudsperson, assessing the legality and proportionality of the decisions and actions of intelligence institutions and intelligence officers.

1. Complaints Related to the Protection of the Rights of Foreign Nationals

Human rights are inherent and universal—they apply to all persons regardless of citizenship or legal status. Depending on the possibility of limitation, human rights are generally classified as absolute and non-absolute rights: absolute rights may not be restricted under any circumstances, whereas non-absolute rights may be limited only in accordance with procedures established by law and in compliance with the principles of legality, reasonableness, and proportionality.

Article 3(1) of the Law on the Legal Status of Foreigners of the Republic of Lithuania (hereinafter – the Law on the Legal Status of Foreigners) provides that foreigners in the Republic of Lithuania enjoy the same rights and freedoms as those established by the Constitution of the Republic of Lithuania, international treaties, laws of the Republic of Lithuania, and European Union legal acts. Paragraph 2 of the same Article further establishes that foreigners in the Republic of Lithuania are equal before the law irrespective of their sex, race, nationality, language, origin, social status, religion, beliefs, or views.

It should be noted that in 2025 the Office received three complaints concerning possible violations of the rights of foreign nationals. One of these complaints related to the possible failure to comply with the time limits established by the Law on the Legal Status of Foreigners. In addition, during 2025, the Office of the Intelligence Ombudsperson received three reports

issued by the Seimas Ombudsperson of the Republic of Lithuania concerning the examination of complaints related to such cases.

Complaints concerning the implementation of rights under the Law on the Legal Status of Foreigners made it possible to identify a potential systemic issue related to the duration of assessments carried out by intelligence institutions regarding potential threats to national security. Such delays directly affect the length of administrative procedures and the legal status of the individuals concerned. As in previous years, a continuing trend was observed whereby assessments issued by the State Security Department regarding potential threats to national security were delayed, which in turn affected the examination of applications submitted by foreign nationals to the Migration Department under the Ministry of Interior of the Republic of Lithuania (hereinafter – Migration Department), resulting in delays in the timely adoption of decisions.

In order to assess the situation, the Intelligence Ombudsperson approached the VSD in 2025. Having evaluated the information received, the Intelligence Ombudsperson identified the reasons for delays in the submission of assessments regarding potential threats to national security, as well as the measures undertaken by the VSD to improve its internal processes in addressing this situation. In light of these circumstances, the Intelligence Ombudsperson proposed considering amendments to the Procedure for Issuing Temporary Residence Permits to Foreigners in the Republic of Lithuania, approved by Order No. 1V-329 of the Minister of Interior of the Republic of Lithuania of 12 October 2005 “On the Approval of the Procedure for Issuing Temporary Residence Permits to Foreigners in the Republic of Lithuania”. Amendments to this procedure would contribute to ensuring a smoother process for the submission of assessments by the VSD regarding potential threats to national security. The Intelligence Ombudsperson will continue to monitor developments relating to this process.

In 2025, as in 2024, complaints concerning the application of the provisions of the Law on the Legal Status of Foreigners most frequently challenged allegedly unlawful actions of the VSD, and disputes arising in such cases were often brought before the courts. However, in such situations, the Law on Intelligence Ombudspersons requires the Intelligence Ombudsperson to refuse to examine the complaint received.

The Intelligence Ombudsperson is the only authority in Lithuania entrusted with the independent oversight of the legality of the activities of intelligence institutions and the assessment of their compliance with the requirements for the protection of human rights and fundamental freedoms. In light of this, the Office of the Intelligence Ombudsperson prepared and submitted to the Seimas of the Republic of Lithuania proposals for amendments to the Law on Intelligence

Ombudspersons. On 13 May 2025, the Seimas registered the draft Law on Intelligence Ombudspersons, which, inter alia, proposes to establish the duty of the Intelligence Ombudsperson to participate in judicial proceedings upon invitation by a court and to provide an expert opinion. These proposed amendments are scheduled to be considered during the 2026 spring session of the Seimas.

2. Complaints Related to Criminal Intelligence

In 2025, the Office of the Intelligence Ombudsperson also received complaints concerning allegedly unlawful criminal intelligence information collection measures applied in respect of applicants, the possible exceeding of the lawful limits of the activities of criminal intelligence authorities, abuse of powers granted to them, and other potential violations of human rights and fundamental freedoms.

As in previous years, during the reporting period some complaints continued to reflect confusion between the concepts of intelligence and criminal intelligence. As a result, applicants approached the Office of the Intelligence Ombudsperson regarding matters

falling outside the competence of the Intelligence Ombudsperson. In such cases, decisions refusing to examine the complaints were adopted in accordance with the Law on Intelligence Ombudspersons. The activities of criminal intelligence authorities are coordinated and their legality supervised by prosecutors and by the heads of the criminal intelligence authorities themselves through internal control mechanisms, while parliamentary oversight is exercised by the Seimas Commission for Parliamentary Oversight of Criminal Intelligence.

In 2025, the activities of the Office of the Intelligence Ombudsperson were not limited solely to the examination of individual complaints. The Office also had a broader systemic impact by identifying potential risks, providing recommendations, and thereby contributing to the implementation of human rights protection standards in the fields of intelligence and counterintelligence.



V. TECHNOLOGICAL CHALLENGES TO PRIVACY AND PERSONAL DATA PROTECTION: IMPLICATIONS FOR THE OVERSIGHT OF INTELLIGENCE INSTITUTIONS

In 2025, the European Commission presented the Digital Package initiative⁴, aimed at simplifying and modernising the European Union's regulatory framework in response to the evolving geopolitical and technological environment. The proposal was presented as one of the measures intended to strengthen the European Union's competitiveness⁵. However, it also attracted criticism due to its potential implications for the right to privacy and the protection of personal data, particularly in situations where such data may subsequently be used for intelligence purposes⁶.

One of the more controversial aspects concerns the provision according to which the further processing of personal data for scientific, statistical, or archiving purposes in the public interest is presumed to be compatible with the original purpose of data collection, without the need for a separate compatibility assessment. This approach has been criticised as creating conditions for the expansion of the purposes of data use, whereby data collected for one purpose may subsequently be used for others. In practice, "scientific" or "statistical" justifications are frequently invoked in the field of national security, for example in the analysis of threats or the identification of behavioural anomalies⁷.

Although the General Data Protection Regulation does not apply directly to the processing of personal data for intelligence purposes, it does apply to the development of technologies that may subsequently be used by intelligence institutions. Consequently, the proposed new rules governing the

processing of special categories of personal data, as well as the possibility of using such data in the development of artificial intelligence systems, give rise to legitimate concerns regarding the protection of human rights both at the stage of technological development and at the stage of practical deployment⁸.

In 2024, the European Court of Human Rights, in *Podchasov v. Russia*, held that weakening end-to-end encryption technologies by creating mechanisms enabling public authorities to gain access to encrypted communications constituted an interference with the right to respect for private life. Although the case concerned Russia, similar debates are also taking place in democratic states⁹.

In 2025, discussions took place within the European Union, as well as in France, Sweden, and the United Kingdom, concerning possible obligations for technology providers to enable law enforcement and intelligence authorities to access the content of electronic communications¹⁰. The creation of such access mechanisms would undermine the very essence of end-to-end encryption namely, that the content of communications can be accessed only by the sender and the recipient and would inevitably weaken the protection of privacy¹¹.

Despite criticism, the European Commission announced its intention to present guidance on encryption technologies in 2026¹². In May 2025, civil society organisations, including the Global Encryption Coalition, publicly expressed concern that such initiatives could create conditions for mass surveillance and could be used as instruments of political pressure

- 4 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024, with a view to simplifying the legal framework for the digital sector (Digital Omnibus Package).
- 5 European Commission Proposes Revisions to GDPR and Other Digital Rules Under Digital Omnibus Package. <https://www.globalpoli-cywatch.com/2025/11/european-commission-proposes-revisions-to-gdpr-and-other-digital-rules-under-digital-omnibus-package/>
- 6 The EU Commission's Digital Package: reforming GDPR, e-Privacy, Data Act, AI, and Cybersecurity. <https://www.reedsmith.com/articles/the-eu-commissions-digital-package-reforming-gdpr/>
- 7 Fantin, Stefano and Vogiatzoglou, Plixavra, Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence (August 21, 2020). Available at SSRN: <https://ssrn.com/abstract=3679850>
- 8 Access to data for law enforcement: Lawful interception. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)775881](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775881)
- 9 Security and Trust: An Unsolvable Digital Dilemma? Europe Must Resist Weakening Encryption for Law Enforcement. <https://www.cep.eu/eu-topics/details/security-and-trust-an-unsolvable-digital-dilemma.html>
- 10 ECtHR, *Podchasov v. Russia*, no. 33696/19, 13 February 2024.
- 11 European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights. <https://www.eff.org/deep-links/2024/03/european-court-human-rights-confirms-undermining-encryption-violates-fundamental>
- 12 Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final.
- A New Era of Attacks on Encryption Is Starting to Heat Up, <https://www.wired.com/story/a-new-era-of-attacks-on-encryption-is-starting-to-heat-up/>
- Swedish Parliament urged to reject law that would "greatly undermine security and privacy", <https://www.statewatch.org/news/2025/april/swedish-parliament-urged-to-reject-law-that-would-greatly-undermine-security-and-privacy/>
- 11 Encryption 'back doors' are a bad idea. <https://www.ft.com/content/186a9bb6-9e62-47ce-b974-ce52a2d73e9f>
- 12 Commission presents Roadmap for effective and lawful access to data for law enforcement, https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en

or repression¹³. In addition, doubts have been raised as to whether weakening end-to-end encryption would in fact contribute to achieving the stated security objectives, since individuals posing threats to society or national security would likely continue to seek alternative secure communication channels. The creation of access keys enabling access to communications protected by end-to-end encryption would inevitably create systemic security vulnerabilities capable of being exploited not only for lawful purposes but also for unlawful ones, thereby weakening overall cybersecurity and diminishing public trust in digital technologies.

In Lithuania, no broader public discussions took place in 2025 regarding access to communications protected by end-to-end encryption or the implications of the Digital Package for the activities of intelligence institutions. However, the Supreme Administrative Court of Lithuania examined a case concerning whether traffic data collected in the course of criminal intelligence activities could be used for the investigation of official misconduct. The Court held that such data could not be used for purposes other than criminal intelligence.

This conclusion is also consistent with the case-law of the Court of Justice of the European Union, according to which electronic communications

traffic and location data may not be transferred to other authorities or used for purposes which, as in the present case, are unrelated to combating serious crime or serious threats to public security¹⁴.

The legal and technological developments discussed above give rise to new challenges for the oversight of intelligence institutions, as they alter the very architecture of intelligence-related information and data collection and use that existing oversight models were designed to supervise. As a result, oversight authorities may increasingly need to move beyond reviewing the lawfulness of individual measures and towards broader systemic oversight encompassing technological design, data-flow chains, and the secondary use of data, in order to ensure that intelligence activities continue to comply with the requirements of legality, necessity and proportionality.

Accordingly, intelligence oversight bodies may increasingly be required not only to assess the lawfulness of specific intelligence-gathering measures, but also to evaluate the systemic compliance of technological solutions, as well as the chains of use and re-use of data collected by intelligence institutions, in order to ensure that intelligence activities continue to comply with the principles of legality, reasonableness and proportionality.

13 Joint Letter on the European Internal Security Strategy (ProtectEU), <https://www.globalencryption.org/2025/05/joint-letter-on-the-european-internal-security-strategy-protecteu/>

14 Judgment of the Court of Justice of the European Union in Case C-162/22, *AG v Prosecutor General of the Republic of Lithuania*.



VI. CHALLENGES

Existing and emerging developments in the fields of intelligence, counterintelligence, and national security give rise to significant challenges for the democratic oversight of intelligence institutions. The rapid deployment of artificial intelligence, machine learning, and bulk data analytics is transforming the capacities of intelligence institutions to collect information, analyse data, and support decision-making processes. While these technologies enhance operational effectiveness, they may also create new risks for the protection of human rights. Consequently, oversight of intelligence services in the future will no longer be limited to assessing legality, reasonableness and proportionality alone. It will also need to encompass substantive assessment of technological solutions themselves, while oversight bodies will need to be systematically strengthened through the development of the necessary technical capabilities and expert knowledge.

Independent intelligence oversight bodies will increasingly need the capacity to understand and assess algorithm-based decision-making systems, the datasets used, and automated risk assessment models. This may require the establishment of specialised algorithm-audit functions or units capable of identifying, in a timely manner, potential biases, systemic errors, or disproportionate impacts on individual rights and freedoms. At the same time, it will be necessary to continuously update the legal framework governing intelligence activities by clearly defining the powers of oversight bodies in the field of technological deployment and ensuring effective and credible oversight mechanisms.

Moreover, the increasing complexity of intelligence activities, driven by technological advances and deepening interinstitutional and international cooperation, requires oversight models that are not only formally comprehensive but also functionally effective, equipped with sufficient powers, expertise, and operational capacity.

In response to these challenges, integrated and independent oversight models combining different oversight functions are gaining increasing prominence in international practice. One such approach is the so-called “end-to-end” integrated oversight model, encompassing all stages of the intelligence cycle. Integrated end-to-end oversight means that an oversight body performs:

- *Ex ante* oversight, involving the assessment of the legality and necessity of proposed intelligence measures prior to their implementation;
- *Ex durante* oversight, encompassing the monitoring of intelligence activities, supervision of the application of authorisations, and assessment of compliance during the implementation of operational measures;
- *Ex post* oversight, involving the review of measures already carried out, their results, legality, proportionality, and potential impact on individual rights and freedoms.

Such an integrated oversight model creates the conditions for a consistent and systematic

assessment of the activities of intelligence institutions, enabling the timely identification of risks and, where necessary, a prompt institutional response. A unified approach strengthens the consistency of oversight activities, enhances the predictability of decisions taken by intelligence institutions, and contributes to the effective functioning of the democratic system of checks and balances governed by the rule of law.

This model is also associated with the professionalisation of oversight through the establishment of institutions possessing a higher degree of expertise in intelligence and counterintelligence matters, stronger analytical and supervisory capabilities, and sufficient operational capacity. This enables oversight bodies not only to perform control functions, but also to provide qualified insights to the executive branch and to act as the “eyes and ears” of parliament.

It should be noted that democratic states address these challenges through different institutional approaches. In the Netherlands, a decision has already been adopted to establish a single integrated and independent body for the assessment and oversight of intelligence and security institutions, combining evaluation, oversight, and complaints-handling functions within one institution. This development reflects an effort to strengthen the consistency and effectiveness of oversight in response to contemporary changes in the security environment.

Another example is the United Kingdom, where an integrated oversight regime has operated since the entry into force of the Investigatory Powers Act in 2016. Its central element is the Investigatory Powers Commissioner's Office (IPCO), which performs prior authorisation review, ongoing oversight, and ex post supervision of the use of intelligence and other investigatory powers. This institution complements parliamentary oversight and judicial complaint mechanisms, thereby ensuring a multi-layered framework of democratic accountability.

It should also be emphasised that the logic of integrated end-to-end oversight is not unique to the models of the Netherlands or the United Kingdom. Different democratic states – including Canada, New Zealand, and Australia – employ systems based on different institutional arrangements that nevertheless collectively encompass ex ante, ongoing, and ex post oversight of intelligence activities. This demonstrates a broader international trend towards ensuring coherent and effective democratic oversight across the entire intelligence cycle, irrespective of the specific institutional architecture chosen.

At the same time, these international examples demonstrate that the integrated end-to-end oversight model constitutes only one of the possible responses to contemporary challenges in the oversight of intelligence activities. The specific solutions adopted depend on each state's constitutional framework, institutional traditions, and chosen model of democratic accountability.



**INTELLIGENCE OMBUDSPERSONS' OFFICE
OF THE REPUBLIC OF LITHUANIA**