Translation from Latvian into English

Data State Inspectorate
Republic of Latvia

DATA STATE INSPECTORATE 2024

ANNUAL REPORT

TABLE OF CONTENTS

ABBREVIATIONS USED IN THE TEXT

Data Law – Personal Data Processing Law

Data Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

DLPDP – project "Establishment of a Distance Learning Programme on Data Protection" (Distance Learning program on data protection)

ECRIS – European Criminal Records Information System

EDPS – European Data Protection Board

EU – European Union

ESF – European Social Fund

ETIAS – European Travel Information and Authorisation System

EURODAC – European dactyloscopy database for asylum seekers

ICT – Information and communication technology

Inspectorate – Data State Inspectorate

OCMA – Office of Citizenship and Migration Affairs

Police Directive – Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

SIS – Schengen Information System

Strategy – Strategy 2021–2025 for the activities of the Data State Inspectorate

TAP Portal – The Unified Portal for the Development of and Agreement upon Draft Legal Acts

N.VIS – National Visa Information System

FOREWORD

Looking back on 2024, I would like to say that it was quite a dynamic year for the Inspectorate and one marked mainly by international cooperation. Various important events and initiatives not only raised public awareness of the protection of personal, data but also strengthened our role both nationally and internationally. The 32nd Spring Conference of European Data Supervisory Authorities, hosted by the Inspectorate, was definitely the highlight of last year. This important event gathered data protection experts from 45 countries in Riga and focused on the role of technology in modern society and its impact on human rights. Technology is neither good nor bad in itself – its impact is determined by how we use it. As data protection authorities, we share the responsibility to innovate in a way that simultaneously promotes development and protects privacy. Only by working with our counterparts in other countries and listening to the needs of the private sector can we ensure that technological development becomes an ally, not a threat or an enemy.

Continuing a tradition started several years ago, last year, we received Estonian and Lithuanian colleagues in Riga. These meetings always serve as a valuable platform for exchanging experiences, strengthening cooperation and developing a joint understanding of common data protection challenges. By joining forces, we address regional issues more effectively and strengthen our position on the European level, too. In 2024, we focused on the results of the joint inspection on short-term vehicle rental that we carried out in close cooperation with our Baltic colleagues.

The Inspectorate's specialists actively participated in other international initiatives, contributing to the expert working groups of the EDPS and representing Latvia at different conferences organised by other countries. In addition, the Inspectorate accepted Moldovan colleagues to share valuable advice and experience on data protection, strengthening cross-border cooperation and promoting a common understanding in this area.

While international cooperation has been successful and vital, our top priority has always been and remains the Latvian people. All our work is focused on educating and raising public awareness about personal data protection, making it an integral part of everyday life. In 2024, we clarified complex data protection issues and also created a dialogue with the public by providing advice and clarifications, gave recommendations and organised several seminars.

This dialogue reminds us of the importance of mutual trust and the significance of every Latvian citizen because it is their understanding and participation that will determine the future of data security in our country.

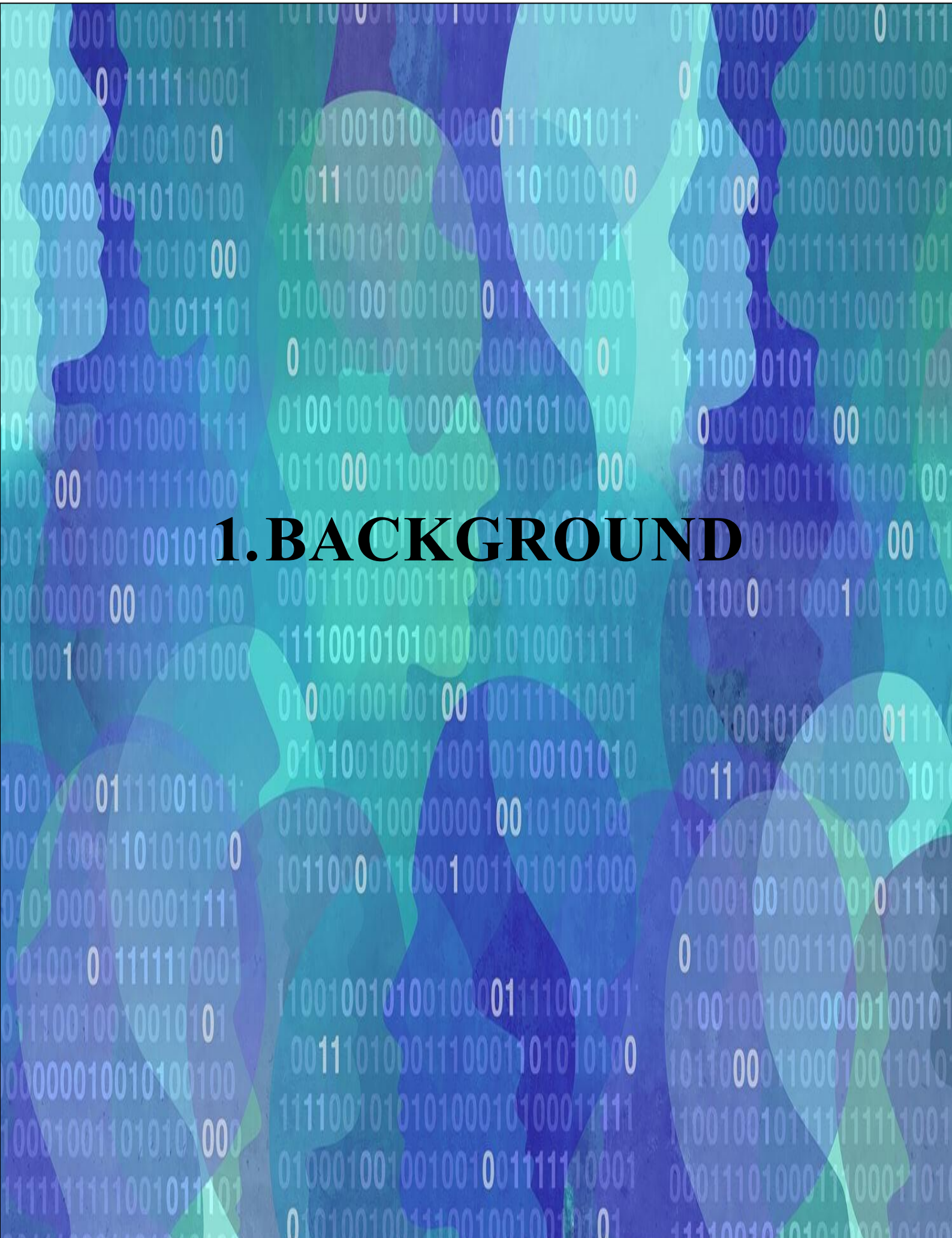
To raise young people's awareness of the value of data and the importance of protecting it, we ran a social experiment to test whether young people value their personal data and to explain what can happen if we recklessly trust others with our data. This initiative was educational and gave us a better understanding of young people's perspectives on privacy and digital security.

In addition, to provide a practical and useful tool for everyone, we have created a free e-learning course "EASY About Personal Data!" Although businesses are the primary audience of this course, it is an excellent tool for anyone concerned about the security and proper handling of their data. All these steps are taken with one goal in mind: to strengthen awareness of personal data protection and to foster a safe and informed society where data security is essential for everyone.

We are now on the cusp of change and looking forward to what 2025 will bring. Either way, our goal remains the same: to continue to raise public awareness of the importance of data protection, to create a safe digital environment and to work to ensure that everyone is confident that their personal data are protected.

Jekaterina Macuka,

Director of the Data State Inspectorate



1. BACKGROUND

1.1. INFORMATION ABOUT THE INSPECTORATE

The Inspectorate was established based on the Personal Data Protection Law[1] and started operating on 1 January 2001.

Under Section 3 of the Data Law, the Inspectorate is an institution of direct administration under the supervision of the Cabinet, which is a data supervisory authority for the purposes of the Data Regulation and carries out the tasks specified in the Data Regulation and other laws and regulations in the field of data processing.

The Inspectorate is a functionally independent institution. The Inspectorate's independence status is determined by Article 52 of the Data Regulation. The independent supervisory authority status is essential for the protection of personal data and the effective exercise of its functions.

The Cabinet exercises institutional oversight through the Minister for Justice. Supervision does not cover the exercise of the tasks and rights assigned to the Inspectorate or the internal organisation of the Inspectorate, including the issuance of any internal regulations, the preparation of reports and decisions concerning the Inspectorate's employees (e. g., decisions on the recruitment and dismissal of employees, transfers and their coordination, secondments, disciplinary proceedings, hearings and disciplinary sanctions).

The Inspectorate ensures the enforcement of the constitutional rights policy in the legal field with regard to the processing of personal data.

The Inspectorate's office is located at 17 Elijas Street, Riga.

1.2. OBJECTIVES AND FUNCTIONS OF THE INSPECTORATE

The purpose of the Inspectorate's activities is to protect fundamental human rights and freedoms in the field of personal data protection, to ensure the representation of the Republic of Latvia before the EU and international institutions within its competence, and to promote the processing of personal data in an efficient, lawful and legally-compliant manner. This objective is also enshrined in the Inspectorate's Strategy and permeates every function and task of the Inspectorate.

The Inspectorate's functions can be divided into two parts: supervision of personal data breaches and prevention.

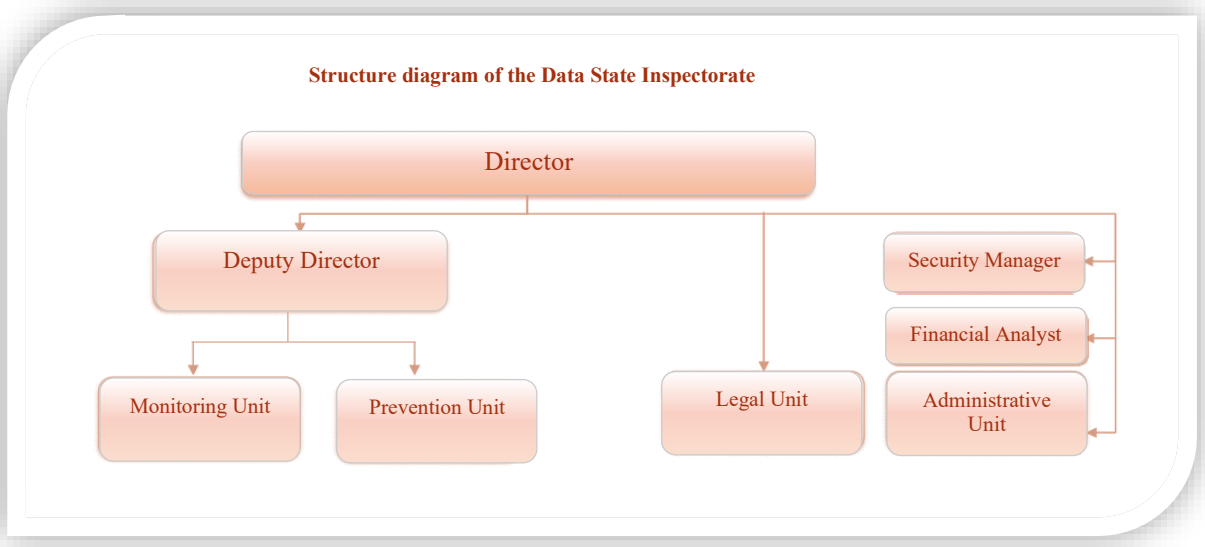
[1] The Personal Data Protection Law expired on 5 July 2018

Based on these functions, the Inspectorate has determined three main lines of action to achieve the objectives determined in the Strategy.

All the lines of action are interlinked and complement each other, contributing both to the further development of each line and to the achievement of the common objective.

The Inspectorate's tasks, which are carried out to ensure the fulfilment of the functions defined in the laws and regulations, can be found **here**.

1.3. STRUCTURE



Since 2023, the Inspectorate has had an Inspectorate Management Group, a collegial body whose purpose is:

1) To ensure the effective implementation of the development and activities of the Inspectorate;

2) To ensure monitoring in line with the Inspectorate's operational strategy and the process approach introduced;

3) To promote the comprehensive involvement and commitment of the Heads of the Inspectorate's Units and staff directly reporting to the Director, in the planning and implementing the Inspectorate's development and activities.

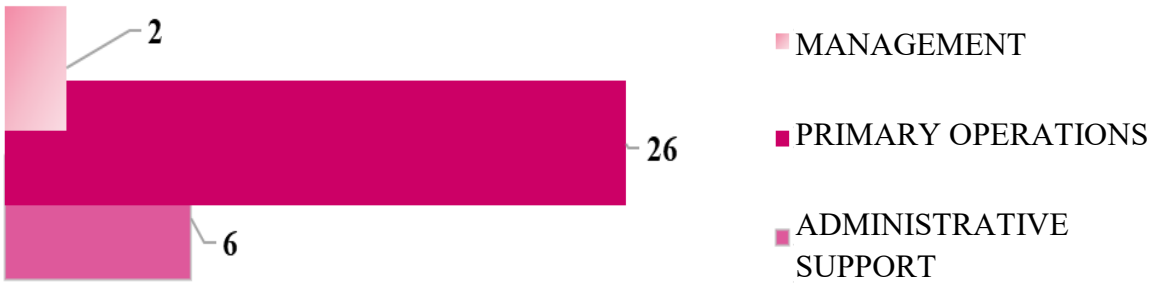
The Inspectorate has an independent Ethics Committee, which, following the procedure under the Code of Ethics of the Inspectorate, examines breaches of the basic principles of professional ethics and violations of the standards of conduct specified in the Code of Ethics.

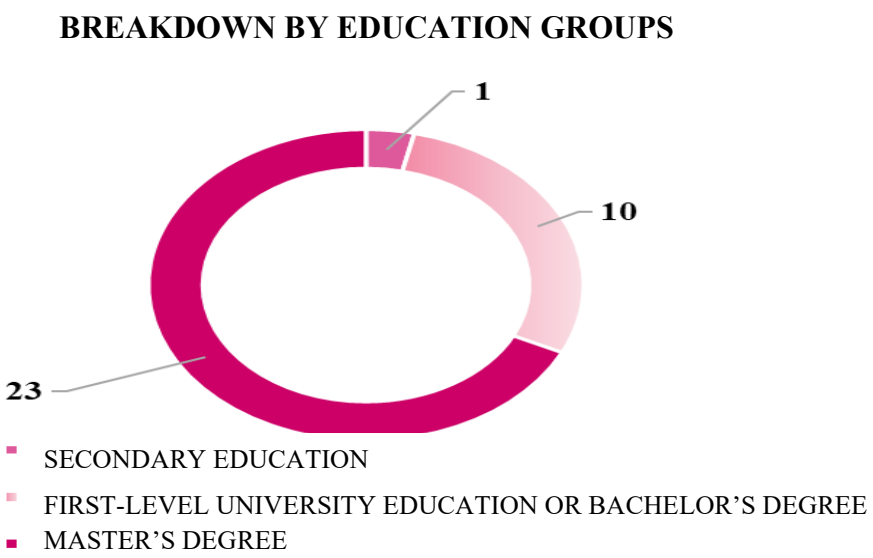
1.4. STAFF

During the reporting period, 35 positions and one fixed-term position were approved in the Inspectorate for the implementation of the EU project DLPDP until 31 January 2025.

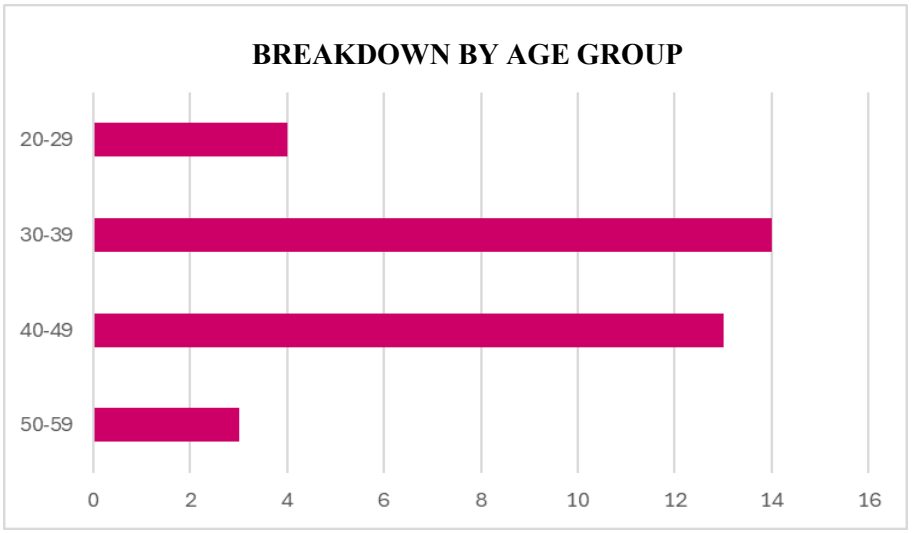
On average, 34 civil servants and employees were employed in the reporting year, of which 27 were women and 7 were men.

BREAKDOWN OF OFFICIALS AND EMPLOYEES BY AREA
(AS AT 31 DECEMBER 2024)



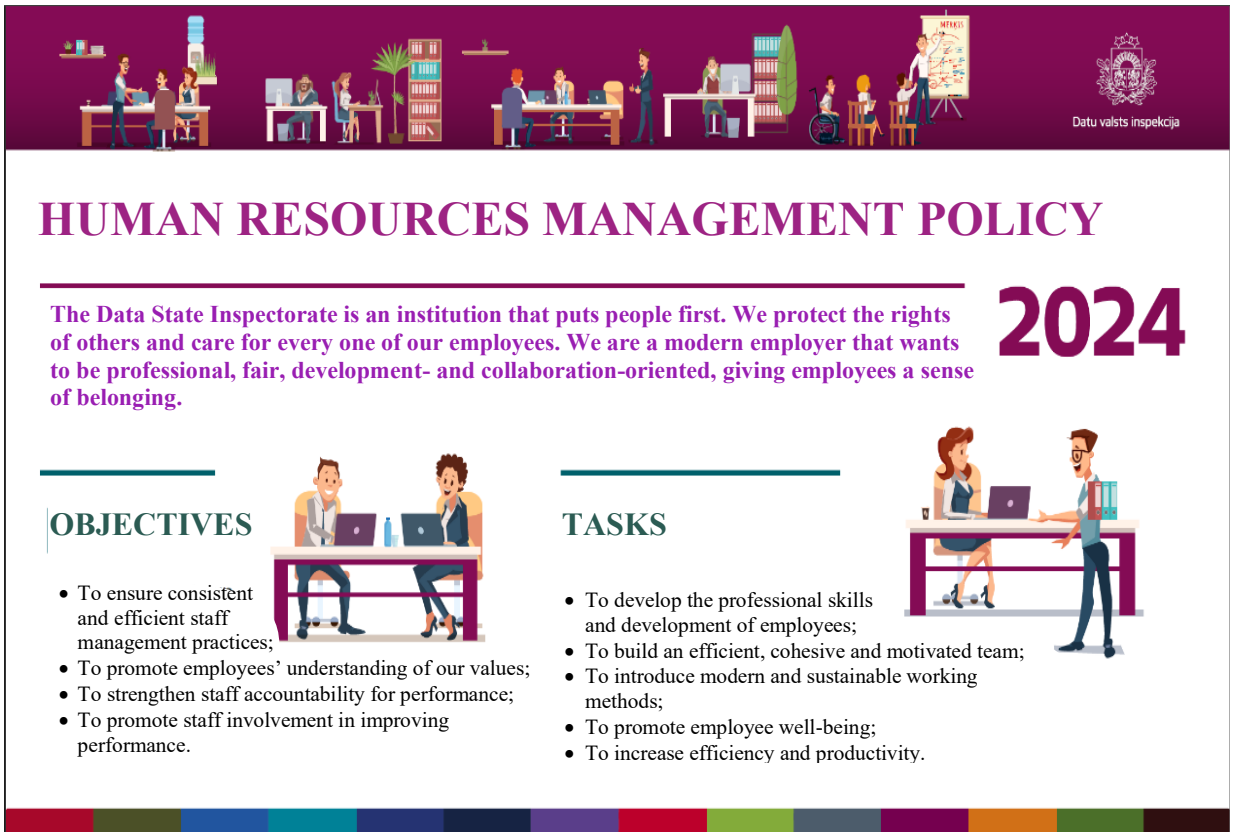


The state civil service relations were terminated for 3 officials and 4 state civil servants were appointed.



During the period under review, the previous working arrangements were maintained, with many employees working in hybrid mode (partly on-site/remote). The Inspectorate, therefore, supports a form of work organisation that allows employees to do their work remotely and to use flexible working time, which promotes work-life balance for the staff.

The Inspectorate has a new Human Resources Management Policy. The policy contributes to achieving the Inspectorate's strategic objectives and long-term development by ensuring the attraction, involvement, motivation, and development of appropriate staff. It also describes the Inspectorate's work culture and is based on the Inspectorate's mission, vision, values and ethics.



FUNDAMENTALS

HUMAN RESOURCES MANAGEMENT POLICY

The Inspectorate is committed to the well-being, safety and health of its employees, creating workplaces that are modern, healthy and comfortable.

The professional and personal development of employees, their knowledge, relevant professional competencies and their skilful application in the performance of their tasks are the Inspectorate's main resources for development. It is, therefore, important for us to promote the learning and professional development of our employees to facilitate their continuous

professional development and the acquisition of new skills for the long-term development of the Inspectorate and to enhance the competitiveness of our staff. We develop leadership and growth in managers to facilitate successful team management and goal achievement. To foster staff development and become an efficient institution with professional staff, a change in learning culture is being introduced.

The content of the Inspectorate's annual training plan is designed to promote the development of staff competencies and to motivate and strengthen the team.

In total, the staff participated in 36 training and exchange events during the year under review to increase the professional competencies, of which 30 were external and 6 internal.

The Inspectorate carried out several employee surveys to create a positive working environment. The results of the surveys are analysed by the management team and action is taken to improve the well-being of employees and the working environment in the Inspectorate.

1.5. INTERNAL CONTROL SYSTEM

The Inspectorate has an internal control system to ensure the successful achievement of its strategic objectives and efficient operation.

To improve the internal control system, amendments to the Inspectorate's risk management rules were adopted in the reporting year, establishing the procedure for identifying, analysing, and assessing risks of corruption, fraud and conflict of interest in the Inspectorate.

A new Data Breach Management Procedure has been adopted, setting out the principles for the classification of data breaches, the persons responsible for data breach management and their scope of powers, the procedures for detecting, reporting, recording, evaluating, and restoring the information system (resource) and for retaining the data breach reports along with the related documents.

The Inspectorate has adopted the Information System Security Policy to specify the guidelines, tasks and principles of the Inspectorate's information system security policy, the principles of the security management organisation and security characteristics and analysis of the system.

1.6. FUNDING AND ITS USE

The Inspection is financed from the following income sources:

1) A grant from the general revenue;

2) Paid services and other own revenue;

3) Foreign financial assistance.

The following is an explanation of the institution's 2024 budget execution by economic classification groups of expenditure, broken down by budget sub-programmes: In 2024, the institution had expenditure in four budget programmes:

- Sub-programme 09.02.00 "Data protection of natural persons";
- Sub-programme 70.15.00 "Implementation of projects and actions under other EU policy instruments (2021–2027)";
- Sub-programme 73.08.00 "Other projects co-financed by foreign financial assistance (2021–2027)";
- Sub-programme 70.21.00 "Repayments to the general budget of the State for the financing of European Union policy instruments (2014–2020)".

No	Financial indicators	Confirmed in law, *euro*	Budget performance, *euro*	
			during the reporting period	in the previous reporting period
A	B	1	2	3
1.	Financial resources to cover expenditure (total)	1,870,531	1,764,709	1,444,423
1.1	Paid services and other own revenue	17,327	6,985	7,929
1.2	Foreign financial assistance	80,152	33,080	39,226
1.3	A grant from the general revenue	1,773,052	1,724,644	1,397,268
2	Expenditure (total)	1,994,753	1,874,679	1,408,990
2.1	Maintenance expenditure (total)	1,994,753	1,874,679	1,399,676
2.1.1	Current expenditure	1,946,226	1,365,627	1,399,630
2.1.2	Subsidies, grants and social allowances	1,455	1,455	0
2.1.3	Reimbursement to the state budget for expenditure incurred	47,072	0	0
2.2	Capital expenditure	0	0	2,802
including by sub-programme:				
09.02.00	**Data protection of natural persons**			
1	Financial resources to cover expenditure (total)	1,664,048	1,623,100	1,526,427
1.1	Paid services and other own revenue	17,327	6,985	13,059

1.2	A grant from the general revenue	1,646,721	1,616,115	1,513,368
2	Expenditure (total)	1,664,048	1,621,353	1,523,162
2.1	Maintenance expenses	1,664,048	1,621,353	1,520,360
2.1.1	Current expenditure	1,664,048	1,621,353	1,520,360
3	Capital expenditure	4,706	0	2,802
70.15.00	**"Implementation of projects and actions under other EU policy instruments (2021–2027)**			
1	Financial resources to cover expenditure (total)	157,160	139,415	117,678
1.1	Foreign financial assistance	31,380	31,380	117,678
1.2	A grant from the general revenue	125,780	108,035	0
2	Expenditure (total)	279,927	250,636	28,362
2.1	Maintenance expenses	279,927	250,636	28,362
2.1.1	Current expenditure	279,927	250,636	28,362
73.08.00	**Other projects co-financed by foreign financial assistance (2021–2027)**			
1	Financial resources to cover expenditure (total)	2,251	2,194	0
1.1	Foreign financial assistance	1,700	1,700	0
1.2	A grant from the general revenue	551	494	0
2	Expenditure (total)	2,251	1,235	0
2.1	Maintenance expenses	2,251	1,235	0
2.1.1	Current expenditure	2,251	1,235	0
70.21.00	**Repayments to the general budget of the State for the financing of European Union policy instruments (2014–2020)**			
2	Expenditure (total)	1,455	1,455	0
2.1	Maintenance expenditure (total)	1,455	1,455	0
2.1.1	Current expenditure	1,455	1,455	0
2.1.2	Subsidies, grants and social allowances	1,455	1,455	0

The institution's state basic budget expenditures in the 12 months of 2024 were EUR 1,764,709, which, compared to 2023, has increased by EUR 120,605 or 7.34%.

The increase in expenditure for the core functions is due to the additional financial resources allocated in the year under review to the priority action "Implementing the General Data Protection Regulation and the functions assigned to it" in the amount of EUR 57,443 and the implementation of the DLPDP in the amount of EUR 250,636. In 2024, the participation of

the institution in the Nordic-Baltic Mobility and Networking Programme (project No PA-GRO-1811) was supported with a budget of EUR 1,235.

For sub-programme 09.02.00 “Data protection of natural persons”, the total revenue increased by EUR 96,673 or 6.33% compared to 2023. Total expenditure increased by EUR 98,191, namely, 6.45% compared to 2023. Expenditure on remuneration increased by EUR 110,818 or 9.16% compared to the previous reporting period, due to the increase in the national base salary and the additional financial resources of EUR 57,443 allocated to the priority action “Implementation of the General Data Protection Regulation and the functions assigned to it” for 2024 under this sub-programme. Expenditure on goods and services decreased by EUR 9,825 or 3.17% compared to the previous reporting period due to the conversion of some face-to-face missions into hybrid meetings and the need to provide only partial funding for the Nordic-Baltic Mobility and Networking Programme project. Capital expenditure decreased by EUR 2,802 or 100.00% compared to the previous reporting period due to the fact that no new computer equipment was purchased to support the institution. In 2024, own revenue from paid services amounted to EUR 6,985 or 40.31%.

For sub-programme 70.15.00 “Implementation of projects and actions under other EU policy instruments (2021–2027)”, the total revenue increased by EUR 21,737 or 18.47% compared to 2023, in line with the implementation schedule of the DLPDP. Total expenditure increased by EUR 222,274 or 783.70% compared to 2023. The remuneration expenditure increased by EUR 16,258 or 57.32% compared to the previous reporting period to ensure that the remuneration of the Head of the DLPDP is in line with the statistical average salary increase of the institution’s staff (legal advisers) as well as with the statistical average salary increase in the country. Expenditure on goods and services increased by EUR 206,016 or 100.00% compared to the previous reporting period due to the full implementation of the contract concluded following a procurement procedure for the “Development, localisation and technical support of the content, interactivity of e-learning “Personal data protection for small and medium-sized enterprises””. On 30 May 2024, a contract was signed to organise the E-learning campaign to promote the E-learning course “Personal data protection for small and medium-sized enterprises”. A successful advertising campaign was implemented in line with the contract requirements until 31 August 2024, ensuring that the promised indicators were met.

On 19 September 2024, the European Commission approved the amendment and extension of the DLPDP until 31 December 2024. Following the extension of the DLPDP grant contract and based on the European Commission’s approval for the preparation of the E-learning course additionally in Lithuanian and Estonian, a contract was concluded on 16 October 2024 to add the content of the E-learning course in these languages. The E-learning course was developed according to the requirements of the contract, with two additional language versions.

The total cost of the DLPDP project is EUR 316,423, of which 90% or EUR 235,356 is EC funding and 10% or EUR 26,151 is national co-financing. Additional funding is needed to cover the non-eligible costs (value-added tax) of the DLPDP in the amount of EUR 54,916. Therefore, the total indicative amount of co-financing required is EUR 81,067. Total national funding (Latvian state budget) for co-financing, pre-financing, and non-eligible costs of the DLPDP is EUR 128,138 (EUR 26,151 for co-financing, EUR 47,071 for pre-financing and EUR 54,916 for non-eligible costs).

For sub-programme 73.08.00 "Other projects co-financed by foreign financial assistance (2021–2027)", total revenue increased by EUR 2,194 or 100.00% compared to 2023, in line with the terms of the Project Contract. Total expenditure, which is also expenditure on goods and services, increased by EUR 1,235 or 100.00% compared to 2023. On 17 May 2024, the Nordic-Baltic Mobility and Network Programme signed a contract for the implementation of project No PA-GRO-1811. Under the contract, the planned project activities must be carried out within one calendar year of notification of the grant decision. In 2024, within the framework of this project, the Inspectorate visited the Finnish Data Supervisory Authority (Tietosuojavaltuutetun toimisto) and the Finnish Ministry of Justice. The purpose of the visit: to share practices on the process of drafting and harmonising external legislation on data protection issues, the role of the data supervisory authority in this process and experience in applying the requirements of Article 6 (3) of the Data Regulation, to discuss current developments in the field of data protection.

The total cost of the project is EUR 4,713, of which 44% or EUR 2,000 is made up of grant funding and 56% or EUR 2,713 is national co-financing.

Sub-programme 70.21.00 "Repayments to the general budget of the State for the financing of European Union policy instruments (2014–2020)" has a total expenditure of EUR 1,455 in 2024. The Inspectorate's project No 786741 – SMOOTH "Delivering the GDPR (Data Regulation) via Cloud Platform Service for Micro-Enterprises" ended in 2021. After the final report was approved, the final payment was received from the foreign partners and transferred to the state budget.

1.7. DELIVERY OF RESULTS AND PERFORMANCE INDICATORS

Name of the indicator	Planned value	Achieved result	Notes
Number of inspections on the processing of personal data	1040	991	Due to staff shortages, it was not possible to carry out all the planned inspections that are becoming increasingly complex. In turn, video surveillance inspections, while less complex, are very time-consuming as they require regular contact with applicants and administrators. Most of the complaints we receive are related to personal conflicts that private individuals try to resolve with the help of the institution.

Number of recommendations developed	3	2	1 Practical video surveillance guidelines for legal entities and co-owners; 2 Guidelines on "Data processing on a large scale".
Educational events (seminars, conferences, workshops) on personal data protection organised (number)	5	11	Based on the Inspectorate's work plan for 2024, 9 online seminars were held for the public on current issues in the processing and protection of personal data, a three-day international Spring Conference was hosted and an information campaign for young people was organised.
The proportion of rulings in favour of the Data State Inspectorate to the total number of court rulings (%)	92	100	In 2024, two court judgements, one in an administrative procedure case and one in an administrative offence case have entered into force. All rulings are favourable to the Inspectorate, so the proportion of favourable rulings is 100%.

Overall, the institution achieved the target value for the performance indicators in 2024.

1.8. KEY OBJECTIVES ACHIEVED

1. The Inspectorate's capacity was reinforced by creating a competitive and favourable working environment and engaging professional and motivated employees in the performance of its functions.

2. The Inspectorate actively participated in the drafting of laws, regulations, and development planning documents and provided 284 opinions in total concerning draft laws, regulations, and development planning documents prepared by other institutions.

3. Practical recommendations for private individuals on video surveillance have been finalised and published and guidelines on large-scale data processing have been developed.

4. A public awareness campaign for young people on the importance of personal data protection has been held.

5. Awareness-raising activities on the processing and protection of natural persons' data, by organising 11 (eleven) events, participating in 15 (fifteen) other events and publishing 54 explanatory notes. The Inspectorate organised an international conference, the Spring

Conference, which brought together representatives of data supervisory authorities from 45 countries for 3 days.

6. Three data protection officer qualification exams were held.

7. On-site inspection was carried out at the Ministry of Foreign Affairs and the Embassy of Latvia in Uzbekistan concerning the compliance of personal data processing with the Visa Information System.

8. A decision was made to issue the first licence for the Customer Due Diligence Tool. It was granted to Salv Technologies OÜ, an Estonian company, for a period of five years.

9. 991 supervisory inspections were carried out and 49 corrective measures were imposed.

2. AREAS OF ACTIVITY OF THE INSPECTORATE

2.1. INSPECTORATE'S INVOLVEMENT IN THE IMPLEMENTATION OF THE DATA REGULATION'S REQUIREMENTS ON THE NATIONAL LEVEL

The quality of national laws, regulations, and policy documents and their compliance with the basic principles for personal data processing is essential to ensure that personal data processing is lawful, that controllers and data subjects can understand their rights and obligations and that the Inspectorate can exercise efficient supervision over personal data processing. Thus one of the tasks the Inspectorate has committed to is contributing to an orderly legal environment.

In 2024, the Inspectorate was actively involved in coordinating draft legislation and policy planning documents to fulfil this task. During the mentioned period, the Inspectorate received 124 new draft laws for coordination on the TAP Portal. In total, 284 opinions have been issued this year (out of which 124 are initial opinions and 160 are repeated opinions). In addition to providing opinions on the TAP Portal, the Inspectorate staff were involved in several working groups and participated in 59 meetings and working groups on draft laws.

In addition to the above, during the reporting period, the Inspectorate, under Sub-paragraph 5.6 of the Cabinet Regulation No 368 of 4 July 2023 "Procedure for monitoring the development activities and liquidation of information systems and information and communication technology resources and services necessary for their operation", provided

31 opinions to the controllers on the development activity descriptions of the national information systems where data processing is carried out, as drafted by them.

During the reporting period, the Inspectorate participated in meetings organised by the State Revenue Service aimed at reviewing the regulatory framework on personal data to be disclosed in the public part of public official declarations, considering the 2023 conclusions of the Ombudsman[2] and the judgements of the Court of Justice of the EU adopted in the last couple of years[3]. The authorities involved in the meetings have never reached a common understanding and solution on proportionate processing of personal data; therefore, the evaluation of the legal framework will continue in 2025.

During the reporting period, the Inspectorate was likewise involved in providing opinions on the draft law "Amendments to the Aircraft Passenger Data Processing Law"[4]. The draft law was drawn up, inter alia, in the light of the findings of the Court of Justice of the EU in its judgement of 21 June 2022 in Case C-817/19 *Ligue des droits humains* regarding the retention period of aircraft passenger data.

In several contributions on this draft law, the Inspectorate drew attention to the findings of the Court in its judgement, namely that it was necessary to distinguish in the legislative framework between the purposes specified in the Passenger Name Record Directive and other purposes not covered by the Directive. Namely, it follows from Paragraph 235 of the judgement that the recorded passenger data cannot be stored in a single database which can be searched for those and other purposes. Namely, storage of these data in such a database would create the risk that these data could be used for purposes other than those referred to in Article 1 (2) of the Directive. It also follows from the Court's findings that the undifferentiated storage of all passenger data is only possible for six months, and this should be clearly reflected in the regulatory framework. At the same time, storage of passenger data beyond the six-month period is allowed where there are objective indications of a risk of terrorist offences or serious crime which would have an objective, at least indirect, link to the flights in question.

Considering that the draft law provides for the processing of passenger data both for the purposes specified in the Passenger Name Record Directive and for the purposes not mentioned in the Directive, namely the prevention of threats to national security, the

[2] Ombudsman's 2023 Inspection Case No 2023-16-5D

[3] Court of Justice of the European Union, in Case C-184/20 and Joined Cases C 37/20 and C 601/20

[4] Draft law No 23-TA-3198

Inspectorate pointed out that the storage periods and their justification should be assessed and specified on a purpose-by-purpose basis. The draft law is currently in the process of inter-institutional coordination.

 During the reporting period, the Inspectorate was involved in the development of the draft law "Law on Biobanks"[5], which provided the processing of personal data of a potential donor. During the period of the coordination of the draft law, the Inspectorate repeatedly issued opinions pointing to the need to align the purposes of processing of personal data specified in the draft law, for which it will be possible to process the donor's biological samples, as well as to distinguish the purpose of the biobank from the purposes of data processing. In addition to the purposes of data processing, the draft law did not clearly define the legal basis for the different data processing activities, i. e., in which cases data processing is carried out based on public interest and in which cases – based on consent.

The Inspectorate also drew attention to the need to clarify the nature of the definition of "dynamic consent" and its difference from consent for the purposes of the Data Regulation. The draft law provided that the controller of a biobank is entitled to process personal data based on an authorisation issued by the institution. The Inspectorate pointed out that Article 6 of the Data Regulation does not provide such legal basis for processing. The draft law is currently in the process of harmonisation and has been submitted to the State Chancellery.

 The Inspectorate also issued opinions on the draft law "Amendments to the Law on the State Aid for Energy Supply Costs"[6], which, inter alia, provided for the exclusion from the law of a provision that provided the development of a functionality for opting out of the processing of personal data. The Inspectorate expressed the view that it would be disproportionate not to ensure the right to opt out from data processing in a situation where the system processes the personal data of the entire population, while in practice, even less than half of the entire population received the benefits. Moreover, as the system is built based on property rather than persons, this inherently led to a situation where the design of the system did not respect Article 25 of the Data Regulation that provides processing by default, i. e., that the controller implements appropriate technical and organisational measures to ensure that only personal data necessary for each specific purpose of processing are processed by default.

[5] Draft law No 22-TA-2110

[6] Draft law No 24-TA-1958

Consequently, the Inspectorate did not see any reason to waive the obligation under Paragraph 2 of the transitional provisions of the law for the State Construction Control Bureau to ensure that household users could opt out of further processing of their personal data in the information system and the possibility to apply for support if they do not wish to do so by 31 December 2024.

In addition, the draft law provided the definition of a new purpose for data processing, i. e., the identification of energy poverty. The Inspectorate pointed out that the processing of personal data of all citizens in the system for a specific purpose would not be proportionate. To identify energy poverty, data could be processed on those individuals who have been granted incentives and thus qualify for this status and not on the whole population. The Inspectorate also pointed out that the Central Statistics Bureau is the central statistical authority in the country. The function of this authority is the provision of official statistics and it has the relevant expertise and the appropriate level of security to perform this function. Consequently, in the Inspectorate's view, it is the Central Statistics Bureau that should be the institution that processes population data to obtain specific statistics on energy poverty.

Against this background, the Inspectorate still sees risks in the draft law in ensuring proportionality in the processing of personal data. In the Inspectorate's view, there is a significant risk that an information system processing a large amount of personal data does not comply with the obligation to ensure data protection by design and data protection by default under Article 25 of the Data Regulation. Despite the Inspectorate's objections, the responsible ministry decided to move the draft law forward for further consideration and adoption.

On 1 August 2024, the Artificial Intelligence (AI) Act came into force, setting the legal framework for the use of AI in the EU. The AI Act is designed to encourage the development of new technologies while balancing the opportunities they offer with the potential risks that may arise in the areas of privacy and the protection of personal data. The Inspectorate actively participated in the drafting of the information report "On the implementation of the requirements of the AI Act", which identifies the responsible authorities, the necessary changes in the laws and regulations and additional resources for the implementation of the AI Act in Latvia. Given that the supervision of the processing of personal data is ensured by the Inspectorate under the Data Regulation and the Data Law, the Inspectorate is designated as the market supervisory authority for the protection of natural persons' data in relation to the AI Act. In 2025, work will continue to implement the requirements of the AI Act.

2.2. MONITORING AND INSPECTING THE PERSONAL DATA PROCESSING

2.2.1. PREVENTIVE INSPECTION ON COMPLIANCE WITH THE PERSONAL DATA PROTECTION REQUIREMENTS IN ORGANISATIONS' PRIVACY POLICIES

In spring 2023, the Inspectorate launched the awareness campaign "Data are valuable – protect them"[7]. The main objective of the campaign was to inform and educate small and medium-sized enterprises on data protection issues from different perspectives. The campaign included the preparation of information materials in the form of articles and explanations, as well as seminars/workshops on privacy policy in different regions of Latvia – Rēzekne, Liepāja, Jelgava, Valmiera, and Riga (which could also be watched online). Moreover, the workshops launched a universal model privacy policy[8] and published presentations and the recordings, raising the issue of the need for a privacy policy.

To further emphasise the importance of privacy policies, and in light of the Inspectorate's observations and the conclusion that controllers have still not paid enough attention to the development of privacy policies and their compliance with the Data Regulation, the Inspectorate organised an online seminar "Privacy Policy and Tips for Developing It"[9] (29 January 2024).

Given that a sufficient amount of educational and explanatory activities has been carried out in the context of the obligation to establish privacy policies, including informing controllers upon request about their obligations under the Data Regulation, the Inspectorate included a task in its 2024 Work Plan to carry out preventive checks on compliance with the personal data protection requirements in the privacy policies of organisations.

Thus, within the framework of the 2024 Work Plan, the Inspectorate carried out a preventive inspection of the privacy policies published on the websites of traders whose core business is mail order or online retail, verifying the compliance of the information contained

[7] Information about the campaign is available here: https://www.dvi.gov.lv/en/data-value-protect-it-campaign

[8] A sample privacy policy is available here: https://www.dvi.gov.lv/lv/dvi#privatuma-politikas-izstrade

[9] A recording of the seminar is available here: https://www.dvi.gov.lv/lv/jaunums/noklausieties-seminaru-par-privatuma-politiku

therein with the data protection regulatory framework. The inspection examined the privacy policies published by 30 companies registered in Latvia to prevent potential breaches and to gain a data-driven understanding of the topic from controllers.

As concerns the obligation to provide information under Articles 13 and 14 of the Data Regulation, after the first inspection of privacy policies, controllers were most likely to provide inaccurate or no information at all on:

- Legal basis for processing;
- Source of the data;
- Persons who will receive the data;
- Duration of data storage;
- Data subject's rights to their full extent.

The published information suggested that the content of the policies was often "borrowed" from foreign websites or websites of other Latvian companies. Privacy policies also provide inaccurate information about the possibility of consenting to privacy policies. Specifically, it states that data processed for other purposes are processed only with the consent of the individual, e. g., "We will not transfer data to third parties without your consent." Similarly, information on data processing is actually included in the policy, but it is not provided substantively, e. g., listing all the legal bases as contained in the Data Regulation, stating that data will be transferred to third parties, and in cases this is possible, the processor's name or business name is not provided. Controllers were not specific in their privacy policies how data subjects can access their information. One controller indicated that it would need a copy of the data subject's identity document and another that the data subject could only exercise their rights in person, even though the company apparently handled all communications online. When informing about the right to complain with the Inspectorate or the supervisory authority, the name or contact details of the Inspectorate were often incorrect (e. g., the registered office address was not updated) or not provided at all.

Data controllers had the least problems with providing their names, contact details and the purposes of the processing.

Within the framework of the inspection, the Inspectorate also assessed how easy it was to find the privacy policy on the website. In most cases, privacy policies were available on the front page of the controller's website, less often under other terms of the controller, e. g., the terms of an online shop or order or alongside a cookie policy.

Overall, the results of the inspection showed that controllers' knowledge of the need for and content of privacy policies is not at a critical level, but that awareness-raising activities are still needed to increase the controllers' awareness and understanding.

2.2.2. PREVENTIVE INSPECTION ON THE PROCESSING OF PERSONAL DATA UNDER CUSTOMER LOYALTY SCHEMES

In July 2024, upon its own initiative, the Inspectorate launched a preventive monitoring of the processing of personal data under customer loyalty programmes. 20 companies were inspected.

During the inspections, all controllers were asked the same questions about their practices in the industry regarding the processing of personal data under loyalty schemes.

The inspections revealed various non-compliances, mainly related to the application of an incorrect legal basis and the setting of storage periods that were too general, which in turn showed that the controller either did not have the necessary knowledge to set retention periods or did not have the knowledge to set appropriate retention periods. The inspections revealed violations of data subjects' rights, mainly related to overly general information and insufficient provision of available information. It also found that companies still lacked a clear understanding of the correct application of the requirements of the Data Regulation.

Overall, the possible non-compliances do not involve significant restrictions of the rights of data subjects in flagrant breach of the requirements of the Data Regulation; however, the recommendations of the controllers on the need for guidance clarifications have been considered as a result of the inspection.

Consequently, the Inspectorate, based on the findings of these inspections, is developing guidelines within its competence on the processing of personal data under loyalty programmes. The guidelines are intended to assist controllers in understanding and organising the processing of loyalty schemes and to facilitate compliance with the requirements of the Data Regulation.

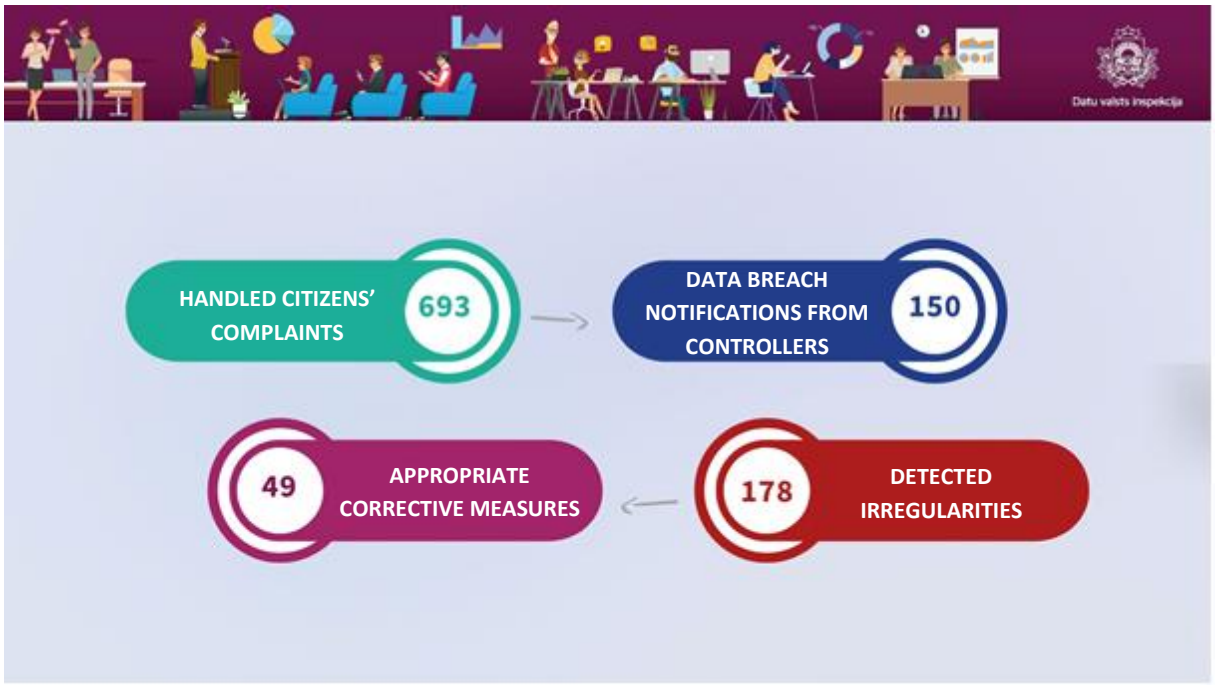
2.2.3. SUPERVISION OF DATA PROCESSING

During the reporting year, the Inspectorate received 693 complaints from the data subjects about possible personal data breaches, 150 notifications from data controllers about personal data breaches, and 148 applications from other third parties (public authorities, organisations, associations) about possible personal data breaches. Based on these complaints,

notifications of personal data protection violations, and the Inspectorate's own initiative, the Inspectorate carried out a total of 991 personal data processing inspections (including initiative inspections) in the framework of administrative proceedings and administrative offence proceedings.

In 203 cases, the Inspectorate had opened an in-depth inspection case, finding 178 infringements, out of which 49 resulted in corrective measures.

The slight increase in the number of inspection cases handled, compared to the previous reporting period, is due to the fact that citizens have become more vigilant and cautious about the security of their data. At the same time, the Inspectorate has observed that the received complaints rarely contain information about systematic breaches by the controller affecting a wider range of data subjects, but are more focused on the individual relationship between the data subject and the controller.



Areas inspected:

- Processing of personal data on online social networks and other websites;
- Video surveillance in public places, private properties, companies and institutions;
- Processing of personal data in the information systems of public authorities;
- Respecting the rights of data subjects;
- Processing of special categories of personal data (including health data);

- Processing of children's personal data;
- Processing of personal data in e-commerce, commercial communications and telecommunications;
- Processing of personal data in the context of out-of-court debt recovery and credit history assessment;
- Processing of personal data by the mass media;
- Processing of personal data using cookies.

2.2.3.1. NUMBER OF COMPLAINTS RECEIVED

The highest number of complaints, 196 out of 693 received during the reporting period, concerned the processing of personal data on online social networks and other websites. In most cases, the processing of personal data was detected, while data subjects were found not to have used the tools available on social networks to delete their personal data; therefore, the data subjects were informed of their right to make a request to the website controller. The second most frequent area of complaint was video surveillance. Given that the technical capabilities of video surveillance cameras are constantly being improved and the equipment is available to a wide range of citizens, there is a tendency for video surveillance cameras to be widely used without citizens being aware of the basic principles of video surveillance. When examining this type of complaint, as in the previous reporting periods, it was found that most often no information signs on video surveillance were displayed or the information sign did not contain all the necessary information required by Section 36 Paragraph Three of the Data Law (name of the controller, contact details, purpose of data processing, as well as an indication of the possibility to obtain other information specified in Article 13 of the Data Regulation).

When examining complaints about video surveillance, Inspectorate officials found that administrators often film a wider area than it is necessary to achieve a specific objective, e. g., filming neighbouring properties. In these cases, the administrators were asked to reduce the surveillance angle.

Compared to 2023, the number of complaints about the processing of personal data in the information systems of public authorities has increased, with a total of 75 complaints received and handled in this regard. Meanwhile, it has been found that citizens increasingly complain about the actions of various healthcare practitioners when viewing personal data in the unified health system ("E-Veselība") without any legally justified reason, i. e., personal data are not viewed within the framework of a treatment episode.

In 2024, the Inspectorate applied corrective measures (order, reprimand) in 49 cases when dealing with complaints from data subjects, calling on controllers to comply with their obligations under the Data Regulation. This included obligations on controllers to comply with the data subject's request, to implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing complies with the requirements of the Data Regulation, to align the personal data processing activities with the provisions on rectification or erasure of personal data or restriction of processing laid down in the Data Regulation.

2.2.3.2. NOTIFICATION OF PERSONAL DATA BREACHES

Under Article 33 (1) of the Data Regulation, in the event of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Inspectorate unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In 2024, the Inspectorate received 150 notifications of personal data breaches, out of which 142 contained information on breach of confidentiality, 4 – on the breach of integrity and 6 – on the breach of availability.

2.2.3.3. DECISIONS TAKEN IN ADMINISTRATIVE OFFENCE CASES

During the reporting period, the Inspectorate made 23 decisions in administrative offence cases; in 20 cases, a fine was imposed on the violator, and in three cases, a warning was issued.

In the year under review, the range of fines imposed in administrative offence cases varied between EUR 100 and EUR 2,000. In 2024, the Inspectorate imposed fines totalling EUR 8,200.

In 14 cases, fines were imposed for offences provided for in Article 83 (5) of the Data Regulation.

In eight cases, a fine was imposed for non-compliance with the basic principles of processing, including the conditions of consent pursuant to Articles 5, 6, 7 and 9 of the Data Regulation (Article 83 (5) (a) of the Data Regulation).

In one case, for non-compliance with an order of the supervisory authority or a limitation on data flows under Article 58 (2) of the Data Regulation or failure to provide access in violation of Article 58 (1) of the Data Regulation (Article 83 (5) (a), (b) and (e) of the Data Regulation).

In five cases, for the controller's failure to provide information to the Inspectorate that it requested and needed to perform its tasks (Article 83 (5) (e) of the Data Regulation).

In 9 cases, the penalty was imposed on the basis of Section 3 Paragraph Four of the Law on Administrative Penalties for Offences in the Field of Administration, Public Order, and Use of the Official Language (failure to provide information, inadequate provision of information, or provision of false information to the Inspectorate).

2.3. CONTESTING AND APPEALING AGAINST DECISIONS TAKEN BY AN OFFICIAL OF THE INSPECTORATE

2.3.1. CONTESTATION

The Director of the Inspectorate has made a total of 14 decisions in 2024. Out of these, five decisions taken by officials were appealed in administrative offence proceedings, while 9 decisions taken by an official were challenged in administrative proceedings.

As regards the appealed administrative offence cases, in all five cases, the Director decided to leave the appealed decision unchanged.

At the same time, with regard to the administrative procedure cases challenged against the Director, it should be noted that six decisions have been adopted to declare the actual conduct lawful, one decision has been made to uphold the decision, one to annul the decision from the date of adoption and one to declare the decision unlawful in part and instruct the relevant Inspectorate Unit to re-examine a specific issue.

One of the most interesting contested cases dealt with during the reporting period was a case concerning a dispute between neighbours over the installation of a smart door peephole (intercom) and its video surveillance. A natural person contacted the Inspectorate with an application claiming that a smart door peephole installed by the neighbour was carrying out video surveillance which did not comply with the requirements of the Data Regulation and asked that the person concerned be held administratively liable.

Having examined the arguments put forward in the application and having heard the other party's explanations, the Inspectorate officer found that the video surveillance in question fell within the exception specified in Article 2 (2) (c) of the Data Regulation, i. e., the activities were carried out in the context of a personal or household activity. Given that the requirements of the Data Regulation were not applicable in the case at hand and that the Inspectorate did not have the competence to examine the case, the case was dismissed.

The natural person contested the institution's *de facto* action to close the case and complained to the Director of the Inspectorate. After examination of the contested application, no new circumstances were found to justify the inclusion of the activities referred to in the original application in the scope of the Data Regulation; therefore, the decision of the Director of the Inspectorate dismissed the complaint. The natural person appealed against this decision in court and the legal proceedings are now at an early stage.

In another case, the question of the right of a healthcare practitioner to have access to the data of a former patient in the unified health information system for statistical purposes was assessed in the context of the appeal stage.

In particular, during the examination of the complaint, the Inspectorate official found the healthcare practitioner guilty of an administrative offence – non-compliance with the basic principles of data processing and accessing the former patient's personal data in the unified health information system without any legal basis.

The healthcare practitioner contested this decision before the Director of the Inspectorate, stating that the access to the data was necessary for statistical purposes, i. e., for the compilation of internal statistics of the medical practice and for the preparation of reports required by the laws and regulations.

The Director of the Inspectorate, after reassessing the case, concluded that the laws and regulations do not oblige a general practitioner to prepare internal statistics. As regards the preparation of the reports, it was concluded that the report did not need to contain the level of detail that the healthcare practitioner had processed. In addition, according to the laws and regulations, a general practitioner is entitled to process all restricted data stored in the health information system about his/her registered patients. Given that the data processed in the case concerned a former patient, no legal basis for processing the personal data of such a patient was established. Consequently, at the appeal stage, the original decision was found to be lawful and well-founded and the challenge application was rejected. The Director's decision was not appealed and has entered into force.

 During the reporting period, another complaint was examined that challenged the Inspectorate officer's inspection and the response received. Within the framework of the inspection, the officer had established that the controller as a natural person had processed (sending notifications by SMS and email) the complainant's personal data (telephone number, email address) and religious data for personal purposes. Consequently, the officer concluded that the processing of personal data and religious data by the controller fell within the exception of Article 2 (2) (c) of the Data Regulation – the processing was carried out in the course of a personal or household event, and consequently did not fall within the requirements of the Data Regulation. The complainant considered that the controller of the particular processing was a legal entity and that the processing would fall within the scope of the Data Regulation.

Upon re-examining the case on its merits, the Director of the Inspectorate concluded that the case established that the processing in question was carried out by a natural person using a telephone number and an email address which are the contact details of a legal entity. The natural person has admitted to using the telephone number and email address for personal use. It also concluded that the administrator and the complainant were personally acquainted, as they had both worked for the same organisation for a long time. In the course of their work in this organisation, they have exchanged contact details. The controller has approached the complainant with SMS messages and emails on religious topics. It also indicates that the communication in question is related to the work of both parties in a particular sphere of private life – the activities and attitudes towards the operation of a particular religious organisation. In view of the above, the Director of the Inspectorate found that the actual action taken by the Inspectorate officer was lawful.

The Director's decision has been appealed in court and the proceedings are currently at first instance.

2.3.2. LEGAL PROCEEDINGS

A total of two final court rulings were issued in the reporting year. Out of these, one ruling was in an administrative offence case and one was in administrative proceedings.

Both of these court rulings are favourable to the Inspectorate.

During the reporting period, an administrative offence case[10] was pending before the appellate instance in connection with the appeal of SIA Tet against the Riga City Court judgement of 20 April 2023. By judgement of the court of appeal of 18 June 2024 in case No 01630000100222.1, the court decided to uphold the decision of the court of first instance and dismiss the appeal.

In its judgement, the court of appeal held, inter alia, that the interpretation of Sections 15 and 16 of the Data Law by the institution and the court of first instance was reasonable. Namely, the employees carried out all procedural actions and these were done by the Inspectorate officials; however, they used data of private individuals; therefore, the claim of SIA Tet that natural persons were involved in the procedural actions is untrue and incorrect.

The court agreed with the institution that SIA Tet had a legal basis to process the personal code corresponding to the name and surname of a specific person in the application; on the other hand, there was no legal basis for processing a third-party personal code because this person, who owned the personal code, did not apply for the service at all, and therefore did not provide data for specific data processing.

The court also found that it was the complainant's conduct, i. e., inadequate risk assessment and failure to comply with the duty of the controller, which contributed to the occurrence of the infringement.

The judgement has entered into force on the day it was prepared and the proceedings are now closed. Thus, SIA Tet was found guilty of an administrative infringement under Article 83 (5) (a) of the Data Regulation; the infringement included also the implementation of a technical solution which allowed the customer, without confirming the contract, to request the Tet+ service on the website using another person's code, without verifying the identity of the recipient of the service.

During the reporting period, the Administrative Regional Court examined the administrative case[11], which was initiated on the basis of the application of Riga Municipality Limited Liability Company "Rīgas satiksme" against the judgement of the Administrative District Court of 30 June 2023 in part.

[10] Administrative Offence Case No 01630000100222.1.

[11] Administrative case No A420188322

In particular, the judgement of the Administrative District Court of 30 June 2023 partially upheld the company's application, declaring unlawful the contested decision in so far as it ordered the applicant to delete the illegally obtained data on the validity period of the COVID-19 revalidation certificate. The remainder of the application was rejected. The applicant appealed against the court's judgement rejecting the application.

The Regional Court thus assessed whether the Inspectorate had reasonably obliged the applicant to delete the vaccination dates obtained and to ensure that information on the reasons for the absence of employees was not available in the drivers' schedule, and whether the remedial measure imposed by the Inspectorate for the infringements – a reprimand – was justified.

In the view of the District Court, the court of first instance was justified in finding that the applicant had processed the vaccination dates of its employees without any legal basis and in breach of the principle of data minimisation. In particular, the court of first instance reasoned correctly why signing the interoperability attestation forms did not constitute explicit consent for the purposes of the Data Regulation. In this context, it is irrelevant whether there were indeed financial consequences for an employee.

The Regional Court also agreed with the court of first instance that the inclusion of the absences in the drivers' schedule did not comply with the basic principles of data processing and was without legal basis. The Regional Court did not find that the provisions of the Labour Law invoked by the applicant provided a basis for including in the schedule information on the reasons for which an employee was absent from work, making it available to all or part of the employees of the company, rather than to the individual employee concerned.

As regards the validity of the imposed remedy, the Regional Court held that the court of first instance had correctly indicated that the purpose of the reprimand was to promote understanding of the rules on data processing contained in the Data Regulation, to ensure compliance with those rules and to prevent a repetition of the infringement. However, the Inspectorate's practice in applying corrective measures, as cited by the applicant, concerns substantially different cases, and therefore the cases cited by the applicant cannot justify a violation of the principle of equality.

Thus, the Regional Court rejected the application of the Riga Municipality Limited Liability Company "Rīgas satiksme". It should be noted that the proceedings in the case continue beyond the reporting period at cassation instance.

2.4. CASE STUDIES

2.4.1. VIEWING PERSONAL DATA IN THE NATIONAL INFORMATION SYSTEM

During the reporting period, the Inspectorate examined several cases concerning the processing of personal data in various state information systems (e-Health, Personal Data Browser and the Information Centre System of the Ministry of the Interior).

In one of the cases, several complaints were received that a doctor's assistant, with user access to health information systems (E-Veselība, Datamed, Doctors' Office) granted to him in the performance of his duties, repeatedly viewed (obtained) the health data of three natural persons known to the doctor's assistant in the systems without any legal basis (i. e., for personal use).

In the case, it was established that the doctor's assistant had made requests for information on the affected person in the systems, thus obtaining (viewing) personal and health data for non-work-related personal purposes outside the framework of healthcare.

Considering all circumstances established in the case, the Inspectorate applied the corrective measure and imposed an administrative fine of EUR 500 on the healthcare practitioner.

2.4.2. PROCESSING OF PERSONAL DATA ON A WEBSITE USING COOKIES

During the reporting period, the Inspectorate carried out inspections in several cases where infringements of the processing of personal data on websites using cookies without an appropriate legal basis were found, thereby violating a number of requirements of the legal framework, including Articles 5, 6, 7 and 12 of the Data Regulation and Section 7^1 of the Law on Information Society Services. Accordingly, the Inspectorate informed the controllers (companies) of the deficiencies and applied the corrective measure in the cases – the obligation to make the necessary changes to the website to remedy any non-compliance within a specific deadline.

In most cases, controllers complied with the remedy imposed, including by responding by the set deadline on the measures taken, which included, depending on the situation, making appropriate changes to the information windows (banners) on cookies and cookie notices in the

privacy policy, as well as reviewing the cookies they use themselves and correcting the mechanism where necessary to ensure that personal data are processed in a way that complies with the legal framework. However, in some cases where the corrective measure was not voluntarily implemented, enforcement continues.

2.4.3. PERSONAL RIGHT TO ERASURE OF DATA

During the reporting period, the Inspectorate inspected the processing of personal data in the context of a publication on a website and of the conduct of the administration of that website in failing to inform the data subject of an action taken at the data subject's request in line with Article 17 of the Data Regulation.

The case concluded that the controller failed to implement adequate and proportionate processing of the data subject's personal data in line with the Data Regulation by making publicly available images of the data subject's face and body on a website more than 11 years after the events mentioned in the publications. Considering the publication in question and the additional circumstances – the data subject's request to erase their personal data and the fact that the controller had not provided the data subject with information on the action taken following the request (or the reasons for not taking action), the Inspectorate found that the data subject's right to privacy and personal data protection was infringed to a greater extent than the rights of the controller and the public and freedom of information.

Overall, the Inspectorate concluded that the processing of the data subject's personal data on the website did not comply with the requirements of Article 5 (1) (a) and (c) of the Data Regulation and Section 32 (1) and (2) of the Data Law, and that the controller did not comply with the requirements under Article 12 (1) of the Data Regulation. Consequently, the following corrective measures were imposed on the controller: (1) reprimanded; (2) obliged to ensure that the processing of the data subject's personal data on the website complies with the Data Regulation by editing or deleting the publications in their entirety; (3) obliged to comply with the requirements under Article 12 (1)–(5) of the Data Regulation, i. e., to comply with the data subject's request and inform the data subject on the activities carried out.

Considering that the controller did not comply with the obligations imposed on him, the Inspectorate officer decided to initiate administrative offence proceedings for non-compliance with the order issued by the Inspectorate and for the continuation of the processing of personal data. For these infringements, the controller was fined EUR 1,000.

2.4.4. PROCESSING OF PERSONAL DATA IN THE WORKPLACE

During the reporting period, the Inspectorate received information on the alleged unlawful processing of personal data in the workplace through video surveillance. The information received showed that the video surveillance camera may also have been equipped with a voice recording function without informing the company's employees.

The inspection revealed excessive processing of personal data on the work premises, in breach of the principles laid down in Article 5 (1) (a) and (c) of the Data Regulation and contrary to Article 6 (1) of the Data Regulation, i. e., the employees' lounge area was under video surveillance. However, the information about the voice recording was not confirmed. As a result, the controller was given corrective action and ordered to change the angle of the CCTV camera.

2.4.5. PROCESSING OF PERSONAL DATA COLLECTED DURING A PROFESSIONAL PHOTO SESSION

The Inspectorate received a complaint that the controller, a professional photographer, had published photographs of the data subject on his website and online social network *Facebook* without the data subject's consent. The inspection revealed that the photographer's website contains photos of individuals (including children) in the "Portfolio" section, some of which also include the names of the individuals, and that the website does not display the necessary information on the use of cookies, despite the use of analytical cookies.

The controller pointed out that the data subject had given his oral consent to the publication of his photographs and that, in his view, the processing of personal data was, therefore, in line with Article 6 (1)(a) of the Data Regulation. However, the Inspectorate concluded that the controller had not demonstrated, following the principle of accountability, that the data subject's consent had actually been (actively) given, and that the consent in this case was, therefore, not in compliance with the requirements of the Data Regulation and was not valid.

At the same time, the Inspectorate concluded that the fee for the photographer's services is conditional on the consent to the processing of personal data, i. e., the publication of the photographs, and, therefore, such consent cannot be considered "free", since the refusal of the processing of data has adverse consequences for the data subject. Moreover, this practice of the

photographer obtaining verbal consent for the publication of his photographs on the website was implemented for all clients. In light of the foregoing, the Inspectorate concluded that the controller had infringed Articles 5 (1) (a), 6 (1) and 7 (1) of the Data Regulation by publishing on his website and *Facebook* photographs of data subjects without their consent.

The Inspectorate also found that the controller did not ensure the option for data subjects to consult the information on the processing before the processing was carried out; thereby, the controller limited access to the exercise of data subjects' rights and infringed Article 12 (1) of the Data Regulation.

In the context of the case, the controller was imposed a corrective measure – a reprimand – and was obliged to establish a data processing policy (privacy policy) on the website.

2.4.6. REPRODUCTION OF PERSONAL DATA

The Inspectorate received a complaint from a natural person about the processing of personal data on a website, stating that she was a healthcare practitioner and that data about her were publicly available in the registers published by the Health Inspectorate and republished on the website of the controller. In its explanatory statement, the controller informed that the information on the website is published using publicly available data based on the Freedom of Information Law.

The source of the published information is the public registers of the Health Inspectorate: Registered healthcare practitioners, healthcare practitioners' jobs and certificates in specialities, and the register of medical establishments. The information published on the website is intended to provide information on the healthcare practitioners, their classification, and certificates and, if a place of work is indicated, the practitioner can be reached by contacting the medical establishment using the telephone number or website address provided.

The Inspectorate pointed out that regardless of the status of personal data as publicly available information, personal data remain personal data and their processing is subject to the provisions of the Data Regulation. Any further processing (including republication) must respect the basic principles of processing under the Data Regulation and be legally justified.

During the inspection, the Inspectorate concluded that the processing (re-publication) of personal data on the controller's website occurs without the legal basis under Article 6(1) of the Data Regulation, and several legal obligations were imposed on the controller to align the processing of personal data with the requirements of the Data Regulation.

2.4.7. PROCESSING OF PERSONAL DATA IN DECISIONS PUBLISHED BY THE INSTITUTION

The Inspectorate examined a complaint of a natural person that the institution when it published a decision on an administrative penalty imposed in an administrative offence case, had provided the following personal data: name, surname and personal code. In the course of the examination of the case, it was found that the institution had later anonymised the personal code by replacing it with symbols in the decision in question. At the same time, it was found that the institution did not have a uniform practice regarding the amount of personal data to be processed (published) when publishing decisions on its website.

The institution acknowledged that the publication of the data subject's personal code was the result of an error, i. e., there was no legal basis for such processing. Consequently, the Inspectorate concluded that in the specific case, the institution had violated Article 5 (1)(a) and (f) and Article 6 (1) of the Data Regulation. As regards the processing (publication) of the names of natural persons – parties to administrative offences, including data subjects – in the institution's decisions, the Inspectorate concluded that it did not comply with Article 5 (1) (a) and (f) and Article 6 (1) (e) of the Data Regulation.

On that basis, the Inspectorate ordered the institution to delete the personal data of the parties (including the data subject, who submitted the complaint) in the decisions published on the website in the administrative offence proceedings.

2.4.8. PROCESSING OF PERSONAL DATA IN THE MEDIA

During the reporting period, the Inspectorate received a complaint from a natural person that a media outlet had over-processed his data. According to the complaint, employees of a company wrote an open letter to the media and the municipality about the alleged unsuitability of the company's manager. The letter was signed by several employees of the company, giving their names and signatures. Upon receiving the letter, the media outlet published an article with the submission, including a list of signatories.

Having examined the case materials, the Inspectorate concluded that the media outlet, by publishing the collective application containing the data of the applicants, had processed personal data in breach of the provisions of Section 32 (2) (1) of the Data Law and in breach of the principles under Article 5 (1) (a) and (c) of the Data Regulation.

In view of the above, the Inspectorate applied a corrective measure and obliged the media outlet to remove the personal data of the signatories of the collective petition from the annex to the publication.

2.5. INTERNATIONAL COOPERATION

2.5.1. ENSURING CONSISTENCY

In 2024, the Inspectorate continued its active involvement in the development of the EDPS working documents. The Inspectorate, as lead rapporteur, continued its work on the preparation of guidelines on the use of anti-money laundering watchlists. The Inspectorate has also been involved as a co-rapporteur in the development of guidelines on the application of the Digital Market Law.

The Inspectorate has also participated in the preparation of other EDPS documents expressing its opinion and providing suggestions.

2.5.2. MONITORING OF EUROPEAN UNION INFORMATION SYSTEMS ON THE NATIONAL LEVEL

In addition to the tasks under the Data Regulation and in line with special laws and regulations, the Inspectorate is obliged to monitor the processing of personal data in EU large-scale IT systems.

To ensure effective supervision over personal data processing, the Inspectorate must carry out complaint investigations, regular audits and other supervisory activities to promote more effective protection of personal data in SIS II, VIS and Eurodac.

In 2024, the Inspectorate continued its preparations for the monitoring of compliance with personal data protection requirements in large-scale IT systems such as ECRIS, ETIAS and system *Satvars*, which are planned to be operational in the near future. The system Satvars ensures interoperability of the data stored and processed in these information systems.

The implementation of the systems has already been postponed several times due to delays in the commissioning of key systems. The planned monitoring activities of the Inspectorate are, therefore, postponed accordingly.

In the meanwhile, the systems already in operation are being monitored with increasing quality; the monitoring activities have been diversified and, together with the growth in the Inspectorate's institutional experience, the performed activities have become more effective.

2.5.3. SCHENGEN INFORMATION SYSTEM

In 2024, an inspection was initiated on the compliance of the alerts entered in the system with the conditions of Chapter VI[12] of the SIS II Decision. Based on the scope of the inspection, it was extended to assess the activities of all parties involved – the SIRENE Latvia Office, the Information Centre of the Ministry of the Interior and the end-user. It is planned to complete the inspection in the first quarter of 2025 by assessing end-user activities with data at category II border control point of the State Border Guard Riga Department in the Riga Port.

A regular inspection was launched on the compliance of the standard replies to data subjects used by the SIRENE Bureau with the laws and regulations governing the operation of SIS II. During the inspection, copies of the used standard replies were obtained and analysed for compliance.

As part of the monitoring activities, the Inspectorate, in cooperation with representatives of the State Police, developed a training programme on the use of N.SIS for State Police officers. The training course operated as part of the National Police College training programmes.

In the next reporting period, the Inspectorate plans to continue cooperation with the State Police to enhance the knowledge and skills of its staff in the field of personal data protection.

2.5.4. VISA INFORMATION SYSTEM

In 2024, an inspection was carried out on the processing of information at one of the N.VIS connection endpoints, the Embassy of Latvia to Uzbekistan. The inspection did not reveal any significant non-compliance with the logical and physical security requirements for the operation of the system. On the basis of the findings, proposals for measures needed to

[12] Regulation 2018/1862 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

operate the system more efficiently are being further developed. In 2024, a plan to address the non-compliances identified during the 2023 inspection has been coordinated and implemented.

A routine inspection was carried out on the compliance of the standard answers used by the OCMA with the legal instrument regulating the operation of the VIS. During the inspection, copies of the used standard replies were obtained and analysed for compliance.

In 2024, the plan to remedy the non-compliances identified during the OCMA audit continued. Measures are launched to monitor the implementation of the plan.

As part of its monitoring activities, the Inspectorate, in cooperation with the State Border Guard, has developed a training programme on using N.VIS for State Border Guard staff.

In the next reporting period, the Inspectorate plans to start cooperation with the Ministry of Foreign Affairs of the Republic of Latvia in developing a training programme on the use of N.VIS.

2.5.5. EUROPEAN DACTYLOSCOPY DATABASE FOR ASYLUM SEEKERS (EURODAC)

During the 2024 monitoring activities, the Inspectorate examined what the relevant authorities have done to remedy the non-compliances identified in the previous audit report and implement the recommended improvements. No deviations from the agreed implementation plan for the additions were identified.

2.5.6. IMPLEMENTATION OF PROJECTS CO-FINANCED BY THE EUROPEAN COMMISSION

In the end of 2021, the Inspectorate submitted a project proposal for the European Commission's financial programme "Citizens, Equality, Rights and Values" (CERV) 2021-2027 under the call for proposals No CERV-2021-DATA for personal data protection supervisory authorities to raise the level of awareness of target groups on data protection rules and their implementation. In March 2022, the European Commission approved the project proposal submitted by the Inspectorate, and in September 2022, the contract for the implementation of the project was signed. The DLPDP aims to develop a distance learning programme on personal data protection for small and medium-sized enterprises, thus providing

this target group with a free tool to acquire knowledge and practical skills in personal data protection and to use the knowledge in their companies.

The DLPDP distance learning programme is available from 1 July 2024. Although the primary audience for the distance learning programme is small and medium-sized businesses, anyone interested in the security of personal data can take the course. The distance learning programme offers: (1) knowledge of data protection and its requirements; (2) practical examples and sample documents for everyday work; (3) self-assessment tests and a certificate upon completion of the final test.

The 2024 distance learning programme was developed in four languages: Latvian, English, Lithuanian, and Estonian. The distance learning programme can be accessed freely or by creating your own profile on the e-learning course website.

The distance learning programme is designed to explain in plain language the provisions of the Data Regulation and to raise awareness of its implementation, the main data protection requirements and the rules for small and medium-sized enterprises (including associations, NGOs, and others) regarding data collection, monitoring, storage, and deletion. It is for everyone – from ordinary employees to board members and company owners.

2.5.7. PARTICIPATION IN THE NORDIC-BALTIC MOBILITY AND NETWORKING PROGRAMME

On 17 May 2024, the participation of the Inspectorate in the Nordic-Baltic Mobility and Networking Programme was supported by the conclusion of a contract for the implementation of project No PA-GRO-1811. The project topic is the sharing of experience and good practices on the involvement of data protection supervisory authorities in the national legislative process. In 2024, within the framework of the project, the Inspectorate visited the Finnish Data Supervisory Authority (Tietosuojavaltuutetun toimisto) and the Finnish Ministry of Justice. The purpose of the visit was to share practices on the process of drafting and harmonising external legislation on data protection issues, the role of the data supervisory authority in this process and experience in applying the requirements of Article 6 (3) of the Data Regulation, to discuss current developments in the field of data protection. In 2025, a visit to the Swedish Data Supervisory Authority is planned.

2.5.8. VISIT BY REPRESENTATIVES OF THE NATIONAL CENTRE FOR PERSONAL DATA PROTECTION OF MOLDOVA (NCPDP)

On 30 and 31 October 2024, the Inspectorate welcomed representatives of the National Centre for Personal Data Protection (NCPDP) of Moldova. The aim of the visit was to strengthen personal data protection practices in Moldova by listening to the Inspectorate's experience and discussing topical issues in the field of data protection. During the visit, the Inspectorate presented the following topics:

- Institute of data protection officer in Latvia;
- Organising the data protection officer exams;
- Assessing the data protection impact in Latvia, explaining how these assessments are carried out and who is obliged to do it. The developed guidelines were also presented.

The visit was part of a joint project between the Council of Europe and the Moldovan institution.

2.6. THE DATA PROTECTION OFFICER

A data protection officer is a knowledgeable person in data protection matters who acts as an assistant and support to the controller or organisation. The duties of a data protection officer may be performed by a person who has passed a qualification examination for data

protection officers organised by the Inspectorate (and included in the list of data protection officers[13]) and by a person who has not passed such an examination but who has sufficient theoretical and practical knowledge in the field of data protection. Similarly, a data protection officer may be appointed either as an employee of the controller, while avoiding any conflict of interest[14], or under an outsourcing or another written arrangement. It should be noted that sometimes people confuse the term data protection officer with the controller, i. e., the person responsible for processing the data. This myth should be debunked because the data protection officer is not directly responsible for the processing, but is an independent person in data protection matters who can analyse the lawfulness of the processing and make suggestions to the controller, who is ultimately responsible for it.

Considering that a person who has passed the qualification examination of data protection officers organised by the Inspectorate can work as a data protection officer, the Inspectorate organised three such examinations in 2024. A total of 36 participants took the examination, and 19 of them passed the examination successfully and were, therefore, included in the public list of data protection officers. Continuing the practice started in 2023, a survey was carried out in in 2024 after each examination and before the results were sent out. This particular order was meant not to influence opinions, to obtain the views of the participants on the organisational and substantive quality of the examination. In general, the participants indicate that the exam was well organised, but some participants have pointed out the need to change the content of the exam and the duration of the exam parts. However, most of the objections are not feasible, as this knowledge test is organised in line with the instructions included in the Cabinet Regulation No 620 of 6 October 2020 Regulations Regarding the Qualification of a Data Protection Officer.

Upon appointment, change and withdrawal of the data protection officer, the controller notifies the contact details of the appointed data protection officer to the Inspectorate[15]. The Inspectorate has set up dedicated forms to facilitate these activities. Noting that sometimes data controllers forget to communicate this information or the information is sent to the Inspectorate by the data protection officer himself, the Inspectorate prepared the explanatory article "What to do after the appointment of a data protection officer". There is no correlation to be confirmed, but it has been observed that in a short period following the publication of this clarification, the

[13] Available: https://www.dvi.gov.lv/lv/datu-aizsardzibas-specialistu-saraksts

[14] The conflict of interest in appointing a data protection officer is explained in more detail here: Qualification of a data protection officer and prevention of conflict of interest

[15] Article 37 (7) of the Data Regulation

Inspectorate received significantly more information from the controllers on their appointed specialists than previously on average over the same period.

In 2024, 46 public sector institutions and 108 private law legal entities announced the appointment or replacement of 154 data protection officers. In some cases, the same controller had appointed more than one data protection officer. Of the appointed specialists, 116 are included in the Inspectorate's public list of data protection officers at the time of their appointment. Information on the appointment or change of a data protection officer is also submitted to the Inspectorate by companies that are not established in Latvia, but whose customers and data subjects may be residents of Latvia.

Considering that Paragraph Five of the Transitional Provisions of the Personal Data Processing Law stipulates that *by 1 June 2024, the Cabinet shall assess the effectiveness of the regulation regarding the qualification examination of data protection officers contained in this Law and submit an assessment regarding the possibility of renouncing this examination to the Parliament*, the Inspectorate, at the request of the Ministry of Justice, provided its statistics- and experience-based, reasoned opinion on the necessity of organising this examination. No changes were proposed to the regulatory framework for the organisation of the examination.

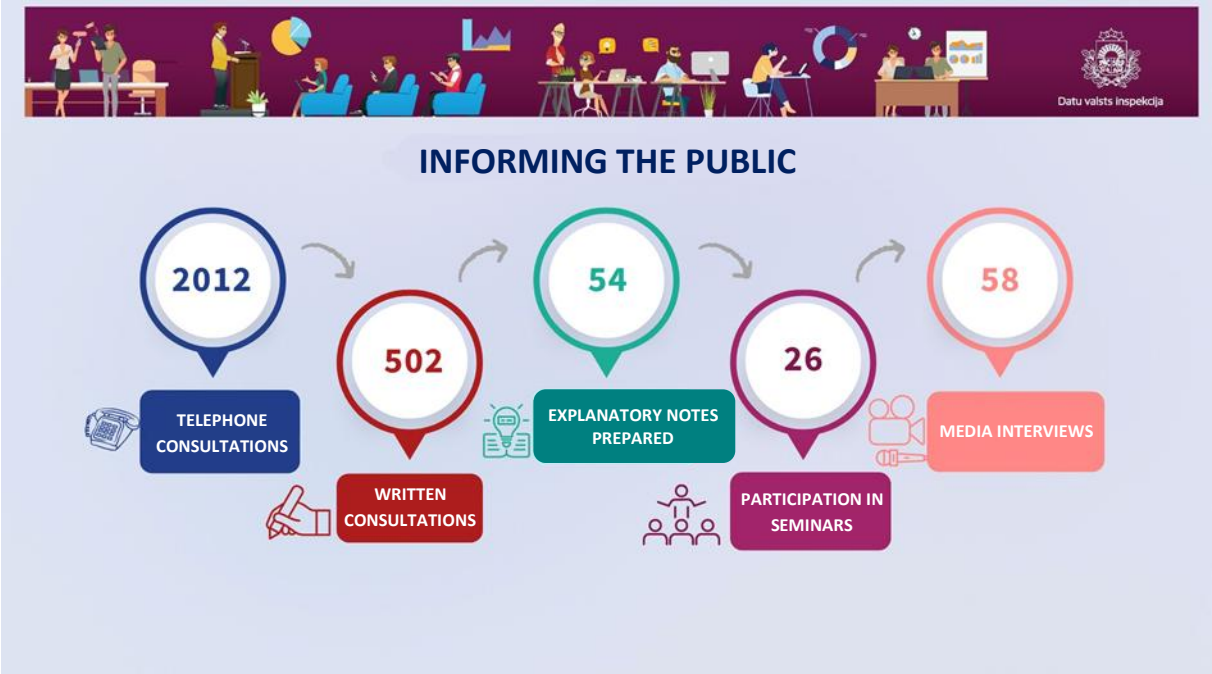
2.7. SUPERVISION OF CREDIT REPORTING AGENCIES

In accordance with the procedure established by the Law on Credit Bureaus and the Cabinet Regulation No 267 of 2 June 2015, Regulations Regarding Licensing and Supervision of Credit Bureaus, two credit reporting bureaus have been registered in Latvia: the joint stock company (AS) "Kredītinformācijas birojs" and the joint stock company (AS) "CREFO birojs". The purpose of the Law on Credit Bureaus is to contribute to the promotion of responsible crediting and responsible and honest borrowing, enabling the formation of personal credit history, and also to ensure legal protection of natural persons to ensure that, upon evaluating creditworthiness, true and complete information is accessible and used. Credit reporting bureaus are licensed and supervised by the Inspectorate. Upon its own initiative and on the basis of the audit report submitted by AS "Kredītinformācijas birojs" and AS "CREFO Birojs", the Inspectorate conducted a preventive inspection on the compliance of personal data processing with the requirements of the Data Regulation and the Law on Credit Bureaus. Overall, this inspection did not reveal any non-compliance with the requirements of the Data Regulation and the Law on Credit Bureaus.

During the reporting period, the Inspectorate provided advice to representatives of credit reporting bureaus on the application of the Law on Credit Bureaus. Also, new council members were assessed following the procedure under Cabinet Regulation No 267 of 2 June 2015 Regulations Regarding Licensing and Supervision of Credit Bureaus.

2.8. COMMUNICATION WITH THE PUBLIC

Communication with the public is a vital part of the Inspectorate's daily work. With the entry into force of the Data Regulation, adopted as of 25 May 2018, the Inspectorate's main task as a supervisory authority is to raise public awareness of the right to privacy and the obligation of those in charge to ensure appropriate technical and organisational measures to respect the secure processing and protection of personal data.



2.8.1 #DVISKAIDRO

For four years, the Inspectorate has been running an informative and explanatory campaign #DVIskaidro (namely, the Data State Inspectorate explains) to provide everyone accessible information on current issues in data protection. It includes weekly explanations with recommendations on how organisations (public and private) can ensure that they are processing data in line with the Data Regulation, and practical advice for citizens on how to exercise their rights. When drafting these explanations, the Inspectorate considers the issues of the moment

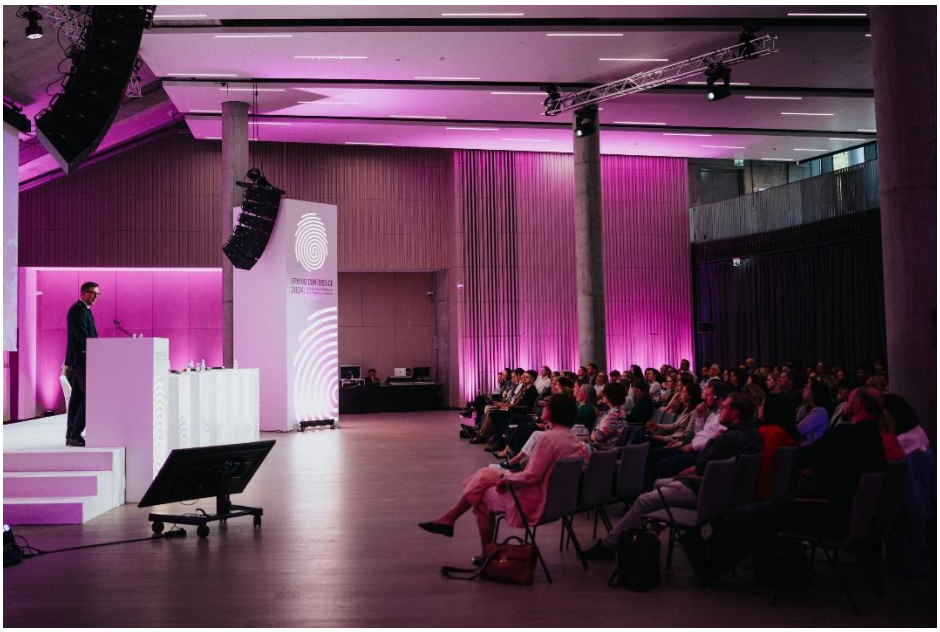
and questions received from citizens, companies, and others. In total, 54 explanatory notes have been prepared for this campaign in 2024.

In the reporting year, the Inspectorate actively cooperated with the media as well, providing 58 answers on the most topical issues in the data protection sector.

2.8.2. SEMINARS

To provide the public information on current developments in data protection and to answer frequently asked questions, the Inspectorate participated in 26 seminars and conferences at the national and international levels, including online seminars on topical issues in data protection: These are some of the key public information events for 2024:

- On **29 January**, marking the 18th European Data Protection Day, an online seminar "Privacy Policy and Tips for Developing It" was held;
- As part of the launch of the seminar series for public administrations, a seminar focusing on the basics of data protection was held on **13 March**;
- From **14 to 16 May**, Riga hosted the 32nd "Spring Conference", bringing together 132 data protection experts from almost all of Europe and beyond;



- On **28 May**, to mark the sixth anniversary of the Data Regulation, an online seminar on "Inspections and Decisions of the State Data Inspectorate" was organised;
- Participation in the "DigiValsts ceļvedis 2024" (Digital Country Roadmap 2024) conference on **5 June**;

- Participation in the data protection professionals' forum Data Protection and Cyber Security as Law Enforcement Core Business in the Hague on **19 September**;

- An online seminar for public administration "Secure Data Transfer" was organised on **28 October**;
- Participation in an employment law forum on data processing in employment relationships on **15 November**;
- A seminar for health workers was organised on **28 November**;
- A seminar for the education sector was organised on **12 December**.

Continuing the practice started in 2022, cooperation with the State Employment Agency to improve the knowledge of unemployed persons continued in 2024. 11 seminars on "Data security and protection in the digital environment" were held where the legal advisor of the Prevention Unit of the Inspectorate explained the essence of data protection, the basics that every data subject should know, especially when staying in the digital environment in the digital age, as well as shared practical examples from the Inspectorate's experience where individuals unknowingly harm themselves by publishing their personal data. The seminars discussed the most popular data protection myths and provided steps to be taken to protect yourself, others and your loved ones from fraudsters, especially those who are less familiar with the written and unwritten laws of the web. A total of 899 clients of the State Employment Agency from all over Latvia attended the seminars. This is the highest number of participants in this seminar-lecture series since its launch. Each seminar concluded with a Q&A session, which led to a discussion on the various challenges of the digital age from the perspective of data protection and

supervisory authority and citizens. Due to the demand from jobseekers and the interest of the State Employment Agency to continue the cooperation, the lecture series will continue in 2025.

More information is available here: https://www.dvi.gov.lv/lv/jaunums/sadarbiba-ar-nva-turpinajas-ari-pern

2.8.3. RAISING PUBLIC AWARENESS, RECOMMENDATIONS AND GUIDELINES

One of the Inspectorate's ongoing and crucial tasks is to inform and educate the public. This is not simply a matter of responding to complaints or informing controllers of their obligations under the Data Regulation or other binding instruments. Nor is it enough to publish the Inspectorate's views on its website. Thus, the Inspectorate, within the framework of its core functions and the functions of a public administration authority, carried out daily education of the population, including foreigners, through telephone consultations, written and face-to-face consultations, public seminars and explanations, participation in events organised by others and media publications.

The Inspectorate also educated the public with Zintis, a virtual assistant available on its website. The assistant's main task is to provide customers with answers to simple, short questions within the institution's competence. In the reporting period, 358 questions were asked to Zintis; however, it should also be noted that some of the questions were not related to the competence of the Inspectorate, and sometimes residents are still learning to understand the nature of a virtual assistant and ask long questions or describe a problematic situation, resulting in an unanswered question. The questions often contain people's personal details, as well as unkind and rude phrases that are automatically recognised.

In 2024, telephone consultations, 502 written consultations and 7 face-to-face consultations were provided. The most frequently explained topics during the consultations were the conditions for conducting video surveillance for natural persons and legal entities, video surveillance without informing data subjects and surveillance of other private property without the owner's consent, data processing on the web and social networking sites, including the processing of cookies and unjustified viewing of data in information systems. In cases of issues, data subjects were explained their rights under the Data Regulation to the protection of their personal data, including addressing the controller.

2.8.4. VIDEO SURVEILLANCE GUIDELINES FOR LEGAL ENTITIES AND JOINT OWNERS

To help legal entities and public authorities comply with the Data Regulation, The Inspectorate has developed guidelines explaining how to carry out video surveillance legally. The Guidelines explain the various legal bases for video surveillance, e. g., legal obligation, public interest and legitimate interest. Examples are also provided to help you understand how to apply the specific legal bases correctly. In addition, the guidelines cover more complex issues, e. g., biometric data processing and video surveillance with the audio function. The guidelines also include model documents to help ensure that video surveillance is carried out legally and in line with best practice, while respecting the principles of personal data protection and safeguarding people's rights.

- Guidelines are available here: https://www.dvi.gov.lv/lv/media/3240/download?attachment https://www.dvi.gov.lv/lv/media/2216/download?attachmenthtt
- Workshop on the guidelines is available here: https://www.youtube.com/watch?v=X3-akFwvmwo
-

2.8.5. GUIDELINES "DATA PROCESSING ON A LARGE SCALE"

The Inspectorate has drafted guidelines on the processing of personal data on a large scale, including criteria to help determine the scale of video surveillance. Video surveillance on a large scale means that processing is carried out over a considerably large area and presents high risks for the processing of human data at regional, national or transnational levels.

- Guidelines are available here: https://www.dvi.gov.lv/lv/media/3408/download?attachment
- Explanation of the guidelines is available here: https://www.dvi.gov.lv/lv/jaunums/dviskaidro-videonoverosana-plasa-meroga-kriteriji-un-nosacijumi

2.8.6. AWARENESS-RAISING CAMPAIGN "DATA ARE VALUABLE – PROTECT THEM" FOR YOUNG PEOPLE

To raise awareness about personal data protection among young people and to encourage them to make informed decisions before sharing their personal data, the Inspectorate organised the campaign "Data are valuable – protect them". The campaign ran from 22 January to 16 June 2024, educating young people about the importance of personal data protection through a variety of activities. The campaign started with the social experiment "All for nothing. Nothing for everything", where on 12, 13 and 14 March, we invited young people to give their personal data in exchange for valuable prizes at AKROPOLE Riga, AKROPOLE Alfa and Galerija Centrs shopping centres. In total, 186 young people aged 13–17 took part in the social experiment. Information and a video on the campaign is available here: https://www.dvi.gov.lv/lv/kampana-dati-ir-vertiba-sarga-tos-jauniesiem

2.8.7. DECISIONS, EXPLANATIONS AND OPINIONS OF THE DATA STATE INSPECTORATE

To inform the public about the processing and protection of personal data and to promote a common understanding of the exercise of natural and legal persons' rights and obligations under the Data Regulation, the decisions taken by the institution on breaches of the requirements of the Data Regulation by controllers and processors, the corrective measures applied, and the opinions and explanations given by the institution in the area of its competence are published on the Inspectorate's website.

The decision database is available here: https://www.dvi.gov.lv/lv/lemumi.

Explanations and opinions are available here: https://www.dvi.gov.lv/lv/skaidrojumi-un-viedokli.

3. PRIORITIES FOR THE NEXT YEAR

1. To continue to strengthen the capacity of the Inspectorate by recruiting professional and motivated staff to carry out its functions. To upskill the workforce by assessing the most strategically important skills to be acquired.
2. To participate in drafting laws, regulations and development planning documents and provide opinions on draft laws, regulations and development planning documents prepared by other institutions that affect matters of personal data protection.
3. To develop guidelines explaining how to carry out a data protection impact assessment.
4. To preventively inspect the processing of personal data by building management companies and the processing of personal data by security companies through video surveillance.
5. To launch a public awareness campaign on data protection for young people.
6. To raise public awareness of the processing and protection of personal data by organising educational seminars (at least eight) and publishing explanations.
7. To fulfil the tasks under Sections 18 to 20 of the Data Law and organise three qualification examinations for data protection officers.
8. In cooperation with the Ombudsman's Office, to develop a clarification on the processing of personal data of State and local government officials for journalistic purposes.
9. To examine the limits of the Inspectorate's scope of authority in matters that likewise concern the police.
10. To develop proposals to improve the tools for implementing the monitoring function by giving the Inspectorate the right to block websites.
11. To draft an opinion on the preconditions and criteria for the use of criminal records in employment relations and propose for the development of a possible regulatory framework in this area.
12. To complete the actions included in the SIS and VIS long-term inspection plan.

Data State
Inspectorate
Republic of Latvia

2025