Data State Inspectorate

OPERATIONAL OVERVIEW

2023

PROFESSIONALISM DEVELOPMENT COOPERATION FAIRNESS OPENNESS

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 (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/EK (General Data Protection Regulation)

DLPDP – Project "Development of a Distance Learning Program in Personal Data Protection" (Distance Learning program on data protection)

ECRIS – European Criminal Records Information System

EDPB – European Data Protection Board

EU – European Union

ESF – European Social Fund

ETIAS – European Travel Information and Authorization System

EURODAC – European Asylum Seeker Fingerprint Database

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 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 prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, repealing Council Framework Decision 2008/977/TI

SIS – Schengen Information System

Strategy – Operational Strategy of the Data State Inspectorate for 2021 - 2025

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

N.VIS – National Visa Information System

FOREWORD

Since the Data Regulation came into force more than four years ago, we have witnessed its important role in giving citizens control over their data while defining clear principles for data processing in both the public and private sectors. The main mission of the Inspectorate – to promote reasonable and responsible personal data processing – is also distinctly reflected in the 2023 Operational Overview. We have monitored compliance with data protection principles, provided support and guidance, and promoted improvements in data processing processes. In 2023, we have distinctly observed that data protection rules are often perceived as a challenge and obstacle to the use of technology, better management and new business opportunities. However, this is not the case, as personal data protection is a human right, and it cannot be an obstacle to anything. Every technology is neutral, therefore, whether it is used in respect of human rights or not, depends on the controllers. We strive to promote this understanding, emphasize the importance of data protection, and show that responsible data processing can foster innovation and business growth. Continuing to pay attention to the fact that information on the processing of personal data is comprehensible to everyone interested and reflects current issues for the public, the Inspectorate held various public information events - seminars and workshops, as well as published informative materials to raise public awareness of the importance of data protection and promote understanding of how personal data is processed.

In 2023, Inspectorate also ensured the reception and evaluation process of the Schengen acquis application evaluation commission in the field of personal data protection, as well as actively monitored the operation of the N.VIS system. The Inspectorate specialists also participated in expert working groups of the European Data Protection Board (EDPB), contributing to the development of guidelines and opinions.

To ensure that personal data protection requirements are taken into account in the development of laws and regulatiions, Inspectorate provided opinions on draft legal acts that affect issues of personal data processing.

Our international cooperation, especially with Lithuania and Estonia, has facilitated effective exchange of experience and a unified approach to data protection issues, strengthening our positions in the European and international arena.

We highly appreciate that during the reporting period, controllers and industry specialists actively consulted with us to ensure appropriate solutions for personal data protection and compliance with regulatory requirements in atypical cases.

We will also actively continue our work in 2024 to educate the public, strengthen international cooperation, and promote the development of new tools and guidelines in the field of data processing. 2023 was a period of growth and development, and we are grateful for the opportunity to work for the benefit of society, protecting personal data and promoting a safe digital environment.

Our work will continue, and we are ready for new challenges and opportunities that await us.

Jekaterina Macuka,

Director of the Data State Inspectorate

1. ACTIVITIES OF THE INSPECTORATE

1.1. INFORMATION ABOUT THE INSPECTORATE

The Inspectorate was established on the basis of the Personal Data Protection Law[1], and started its operation on January 1, 2001.

In accordance with Section 3 of the Data Law, Inspectorate is an institution of direct administration under the supervision of the Cabinet which is a data supervisory authority within the meaning of the Data Regulation and carries out the tasks in the area of data processing specified in the Data Regulation and other laws and regulations.

The Inspectorate operates as a functionally independent institution. The independence status of the Inspectorate is provided for in Section 52 of the Data Regulation. The status of an independent supervisory authority is a crucial component in the protection of personal data and the effective execution of functions.

The Cabinet shall implement institutional supervision through the Minister for Justice. Supervision does not apply to the implementation of the tasks and rights assigned to the Inspectorate, as well as issues of the internal organization of the Inspectorate, including the issuance of internal regulatory acts, preparation of inquiries and decisions relating to the employees of the Inspectorate (for example, decisions on the hiring and dismissal of employees, transfer and its coordination, sending on a business trip, initiation of disciplinary cases, examination and application of disciplinary penalties).

The Inspectorate ensures the implementation of constitutional rights policy in the field of law, in relation to the processing of personal data.

The Inspectorate Office is located in Riga, Elijas iela 17.

1.2. INSPECTORATE'S OBJECTIVES AND FUNCTIONS

The aim of the operation of the Inspectorate is to protect fundamental human rights and freedoms in the area of data protection, to ensure the representation of the Republic of Latvia in the European Union and international institutions within its competence, and to facilitate that the processing of personal data is carried out efficiently, legally and in accordance with

[1] The Personal Data Protection Law ceased to be in effect on July 5, 2018

legislation. This objective is also reinforced in the Inspectorate Strategy and is observed in performing every function of the institution or planning tasks to be carried out.

The functions of the Inspectorate can be conditionally divided into two parts – supervision over personal data breaches and a preventive function.

Based on these functions, in order to achieve the goals set out in the Strategy, the Inspectorate has identified three main areas of operation.

1. **Informed, motivated society and violations prevented in a timely manner.**

Within this operational direction, the recognition of the institution in society is promoted, both increasing the public's understanding of their rights in the field of personal data processing and the understanding of those who process personal data about their obligations. Also, within the framework of the direction, measures are implemented to promote the provision of a unified approach regarding the provision of personal data protection measures, by developing guidelines, recommendations, explanations, as well as binding public administration regulations.

The mentioned operational direction is particularly important, as only an informed society is capable of effectively exercising its rights, while informed controllers are capable of effectively fulfilling their duties. As a result of the mutual voluntary implementation of their rights and obligations, data processing violations are identified and eliminated in a timely manner, and the rights to personal data protection are ensured in the most effective way without the direct involvement of the supervisory authority.

2. **Effective personal data monitoring ensured.**

Within this operational direction, it is ensured that the decisions and penalties applied by the Inspectorate are transparent, clear, and fair. As a result, data controllers are motivated to comply with the personal data processing requirements set out in laws and regulations.

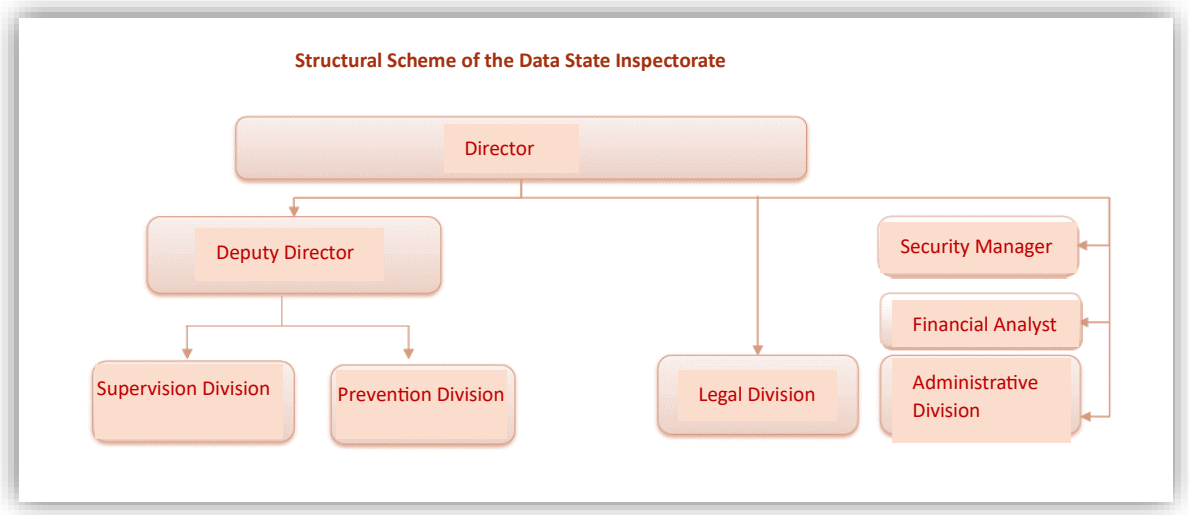
3. **An effective and development-oriented institution.**

Within this operational direction, the institution purposefully moves towards a value-based organizational culture, at the center of which is a human and work for the benefit of society. The values of the Inspectorate – professionalism, development, cooperation, fairness, and transparency – promote the achievement of the Inspectorate's mission and vision, shape the organization's environment and culture, determine the perception and thinking of employees, which is reflected in the actions and attitudes of each employee, promote resource dedication, enhancing employee professionalism, and establishing effective communication channels with the public.

All operational directions are interconnected and complementary, both promoting the further development of each individual direction and achieving the common goal.

You can familiarize yourself with the tasks carried out by the Inspectorate to ensure the performance of functions specified in regulatory enactments **here**.

1.3. STRUCTURE



Since March 2023, the Inspectorate Management Group has been operating within the Inspectorate; it is a collegial institution whose aim is to:

1) ensure effective implementation of the Inspectorate's development and operations;

2) ensure supervision in accordance with the Inspectorate's operational strategy and the implemented process approach;

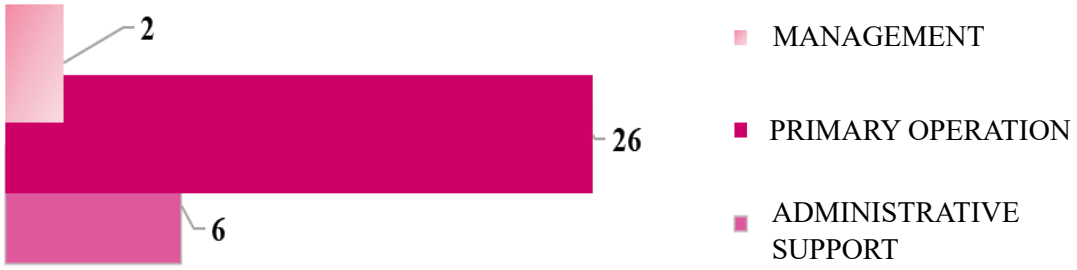
3) promote comprehensive involvement and engagement of the Inspectorate Unit leaders, as well as employees directly subordinate to the Director, in the planning and implementation of the Inspectorate's development and operations.

The Inspectorate has an independent Ethics Committee, which, in accordance with the procedure laid down in the Code of Ethics of the Inspectorate, examines violations of the basic principles of professional ethics and standards of conduct set out in the Code of Ethics.

1.4. STAFF

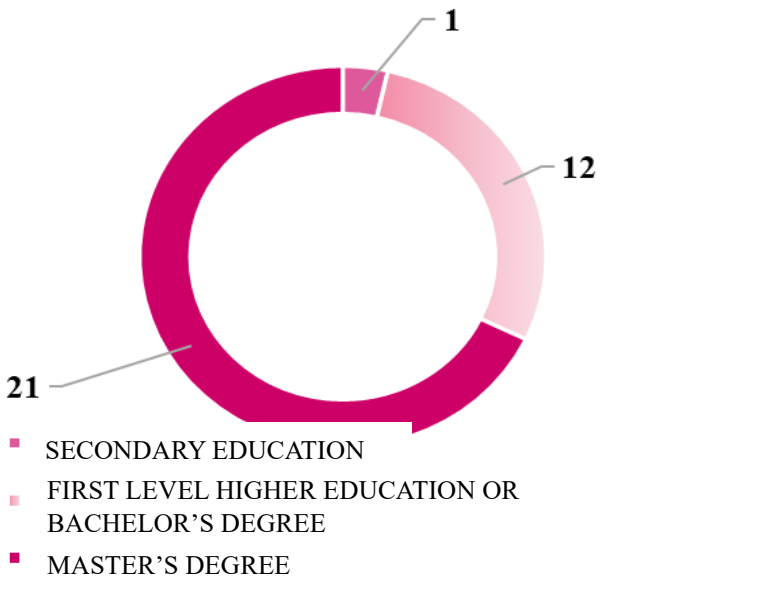
During the reporting period, the Inspectorate confirmed 35 permanent positions and one temporary position for the implementation of the European Union project DLPDP until September 30, 2024.

DIVISION OF OFFICIALS AND EMPLOYEES BY AREA
(as at 31.12.2023)

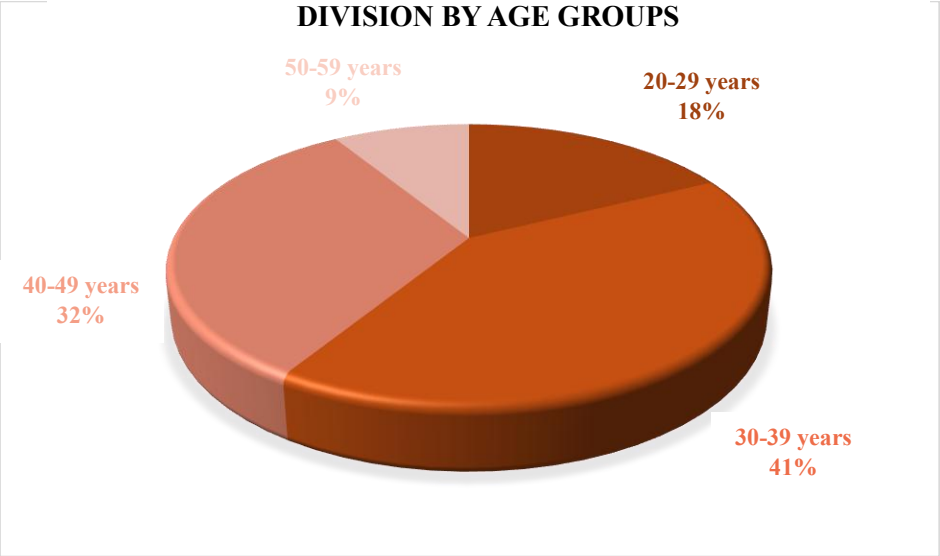


On average, 34 officials and employees are employed in the reporting year, of which 26 are women and 8 are men.

DIVISION BY GROUPS OF EDUCATION



Civil service relations were terminated with 3 officials and legal employment relations with 3 employees. 5 civil service officials were appointed, and legal employment relationships were established with 3 employees.



During the reporting period, the previously introduced work organization was maintained, where many employees worked in a hybrid mode (partly in-person/remotely).

The Inspectorate has established and implemented a new remuneration system. The remuneration system is based on principles that motivate employees to achieve objectives, encourage employee development and growth, and foster employee loyalty to the Inspectorate. The following principles have been observed in determining the monthly salaries of employees:

- **fairness**: a similar monthly salary is determined for work of the same or similar value, qualifications and competences and work performance;
- **transparency**: the procedure for determining the employee's monthly salary level is available to all employees of the Inspectorate and is explained as necessary;
- **orientation to the result**: the essence of the individual monthly salary criteria is to adequately reward the employee's investment (qualifications and competences), result (quality work performance), to promote their constant increase, so that the monthly salary of each employee corresponds to his or her investment and work results;
- **flexibility:** in accordance with the changes in the assessment of the criteria of the individual monthly salary of the employee, the individual monthly salary of

the employee is regularly revised, taking into account the possibilities of the salary budget of the Inspectorate.

Changes are being introduced in the learning culture to promote employee development and become an effective institution with professional employees.. The content of the Inspectorate's annual training plan is designed to promote the development of employee competencies, as well as to motivate and strengthen the team.

Overall, to enhance professional competence, the staff ensured participation in 18 training qualification events during the reporting year, of which 14 were external trainings and 4 were internal trainings.

To create a favorable working environment, several employee surveys were conducted at the Inspectorate. The survey results were analyzed in the management group, and actions were taken to improve the well-being and work environment of the employees in the Inspectorate.

1.5. INTERNAL CONTROL SYSTEM

An internal control system has been established to ensure the successful achievement of strategic goals and effective operation of the Inspectorate..

In the reporting year, the rules of risk management of the Inspectorate have been developed and adopted, establishing a uniform procedure for risk management in the Inspectorate, risk management duties and division of responsibility.

The review of the Inspectorate's core operational processes (service implementation), management processes, including performance evaluation management processes, administrative support processes, and resource provision support processes has been completed, and procedures for their further review and improvement have been established.

At the beginning of the reporting year, the security policy of the Information Systems of the Inspectorate was adopted regarding the information systems used in the Inspection and information processing/storage locations. The mentioned document sets out the basic guidelines of the security policy and the principles of the security management organization, the characteristics and analysis of the system in the field of security, as well as the principles of security.

The Inspectorate's Communication Technology Development Strategy 2023-2025 has also been adopted, which sets out the main directions of the Inspectorate's ICT development, as well as the objectives to be achieved for the period.

1.6. FUNDING AND ITS USAGE

The funding for the Inspectorate is made up of the following revenue sources:

1) grant from general revenues;

2) paid services and other self-generated incomes;

3) foreign financial aid.

Below is an explanation of the Inspectorate's 2023 budget execution for expenditure by economic classification groups divided by sub-programs of the budget. In 2023, the Inspectorate had expenses in two budget programs:

- sub-program 09.02.00 "Personal Data Protection";
- sub-program 70.15.00 "Implementation of projects and actions under other EU policy instruments (2021-2027)".

No.	Financial indicators	Approved by law, *euro*	Budget execution, *euro*	
			during the reporting period	during the previous reporting period
A	B	1	2	3
1.	Financial resources for covering expenses (total)	1,664,258	1,644,105	1,444,423
1.1.	Paid services and other own incomes	17,327	13,059	7,929
1.2.	Foreign financial aid	117,678	117,678	39,226
1.3.	Grant from general revenues	1,529,253	1,513,368	1,397,268
2.	Expenses (total)	1,697,709	1,551,524	1,408,990
2.1.	Maintenance expenses (total)	1,693,003	1,548,722	1,399,676
2.1.1.	Current expenses	1,693,003	1,548,722	1,399,630
2.2.	Subsidies, grants and social benefits	0	0	46
2.2.1.	Social payments and compensations	0	0	46
3.	Capital expenditure	4,706	2,802	9,314
including by sub-programme:				
09.02.00	**Personal Data Protection**			
1.	Financial resources for covering expenses (total)	1,546,580	1,526,427	1,402,837
1.1.	Paid services and other own incomes	17,327	13,059	7,929
1.3..	Grant from general revenues	1,529,253	1,513,368	1,394,908
2.	Expenses (total)	1,546,580	1,523,162	1,400,855

2.1.	Maintenance Expenses	1,541,874	1,520,360	1,391,541
2.1.1.	Current expenses	1,541,874	1,520,360	1,391,495
2.2.	Subsidies, grants and social benefits	0	0	46
2.2.1.	Social payments and compensations	0	0	46
3.	Capital expenditure	4,706	2,802	9,314
70.15.00	**Implementation of projects and actions under other EU policy instruments (2021-2027)**			
1.	Financial resources for covering expenses (total)	117,678	117,678	41,586
1.2.	Foreign financial aid	117,678	117,678	39,226
1.3.	Grant from general revenues	0	0	2,360
2.	Expenses (total)	151,129	28,362	8,135
2.1.	Maintenance expenses	151,129	28,362	8,135
2.1.1.	Current expenses	151,129	28,362	8,135

The expenses of the state basic budget of the Inspectorate in the 12 months of 2023 were 1,644,105 *euros*, which, compared to 2022, have increased by 199,682 *euros* or 13.82%.

The increase in expenses for the implementation of basic functions is related to the fact that in the reporting year additional financial resources were allocated to the priority measure "Application of the General Data Protection Regulation and provision of the functions imposed by it" in the amount of 104,551 *euros*, as well as the implementation of the Inspectorate project DLPDP in the amount of 28,362 *euros*. In the reporting year, capital investment expenses were lower because computer equipment was purchased to replace the remaining worn out computer equipment.

For sub-programme 09.02.00, the total revenues of "Personal Data Protection" increased by 123,590 *euros*, 8.81%, compared to 2022. Total expenses, compared to 2022, increased by 122,307 *euros*, 8.73%. Expenditure for compensation compared to the previous reporting period increased by 135,111 *euros* or 12.57%, which is related to the increase in the basic salary in the country and the additional financial resources allocated for the year 2023 within the framework of this sub-program for the priority measure "Application of the General Data Protection Regulation and provision of its imposed functions" in the amount of 104,551 *euros*. Expenditure for goods and services, compared to the previous reporting period, decreased by 6,246 *euros* or 7.58% due to the fact that some face-to-face business trips were transformed into hybrid meetings. Capital expenses, compared to the previous reporting period, decreased

by 6,512 *euros* or 69.92% due to the fact that new computer equipment was purchased for the provision of the institution instead of the remaining worn out computer equipment. In 2023, the implementation of own revenues from paid services reached 13,059 *euros* or 64.70%.

For sub-programme 70.15.00 "Implementation of projects and actions under other EU policy instruments (2021-2027)", total revenues (foreign financial assistance) increased by 76,092 *euros* or 182.98% compared to 2022, according to the initial schedule of the Project implementation. Total expenses, which are also expenses for remuneration, compared to 2022, increased by 20,227 *euros* or 248.64%. The mentioned expenses increased to ensure compensation for the Project Manager in accordance with the average statistical salary increase of the institution's employees (legal consultants), as well as the average statistical salary increase in the country. Expenditure for goods and services, compared to the previous reporting period, decreased by 3,448 *euros* or 100.00%, as a result of the procurement procedure; the contractor did not request the advance provided in the contract for "E-learning "Personal data protection for small and medium enterprises" content, interactivity development, localization and technical support " and the entire amount provided in the contract will be paid after the completion of all works in 2024. The implementation period of the project is from September 1, 2022 to August 31, 2024, and the institution is the sole implementer of the project.

The total cost of the project is 316,423 *euros*, of which 90% or 235,356 *euros* is EC funding, and 10% or 26,151 *euros* is national co-financing. In addition to that, funding is needed to cover the ineligible costs (value added tax) of the DLPDP project — 54,916 *euros*. Therefore, the necessary indicative co-financing totals 81,067 *euros*. In total, an indicative amount of 128,138 *euros* must be provided from national funding (Latvian state budget funds) for co-financing, pre-financing and covering non-eligible costs of the DLPDP project (26,151 *euros* for co-financing, 47,071 *euros* for pre-financing and 54,916 *euros* for covering non-eligible costs).

PERFORMANCE OF RESULTS AND THEIR PERFORMANCE INDICATORS

Indicator name	Planned value	Execution	Explanation
Number of personal data processing audits	1,040	955	Due to staff shortages, it was not possible to carry out all planned inspections, as they become more complex. Meanwhile, although video surveillance checks are not so complex,

			they are time-consuming as they require maintaining regular correspondence with applicants and controllers. This is because the majority of complaints are related to personal conflicts, which individuals try to resolve through the mediation of the institution.
Number of recommendations developed	3	2	1. Recommendation "Processing of personal data in the field of telemarketing as a processor"; 2. Development of privacy policy, including a sample privacy policy template.
Organized educational events (seminars, conferences, workshops) on personal data protection (number)	5	8	Based on the institution's work plan for 2023, six online seminars have been organized for the public on current issues in personal data processing and protection. In collaboration with the Patent Office, participation in the discussion festival "LAMPA" was ensured – a discussion "A frivolous date with serious consequences". Within the framework of the campaign "Your data – Your safety", seminars/workshops were organized in various regions of Latvia.
Percentage of favorable decisions for the Data State Inspectorate against the total number of court decisions (%)	92	100	In 2023, 6 court judgments came into force in the APL procedure. All decisions are favorable to the Inspectorate; therefore the proportion of favorable decisions is 100%. 2 court judgments in favour of the Inspectorate have entered into force in the administrative offense process. Therefore, the proportion of favorable decisions is 100%.

Overall, in 2023, the institution has achieved the planned value of performance indicators.

1.7. THE MAIN GOALS ACHIEVED

During the reporting year, several tasks essential for the development of the institution and the protection of the right to personal data processing were set and carried out.

1. Strengthen the Inspectorate's capacity by creating a competitive and favorable work environment within the Inspectorate, attracting professional and motivated employees to ensure the execution of the Inspectorate's functions.

2. There has been active involvement in the development of drafts of laws and regulations and development planning documents and a total of 274 opinions have been given on the drafts of laws and regulations and development planning documents prepared by other institutions.

3. Accreditation criteria for code of conduct monitoring bodies have been published.

4. Preventive inspections have been carried out on the compliance with personal data protection requirements in the field of telemarketing in relation to the activities of data controllers, an annual supervision inspection in credit information bureaus, a survey of data controllers who are obliged to appoint a data protection officer, as well as the completion of the Baltic States inspection in the field of short-term vehicle rental.

5. A public information campaign for small and medium-sized companies in the field of data protection has been implemented.

6. Measures have been taken to promote public understanding of the processing and protection of personal data by organizing eight educational seminars and publishing 43 explanations.

7. An on-site inspection was carried out at the Ministry of Foreign Affairs and the Latvian Embassy in Kazakhstan regarding the compliance of personal data processing with the Visa Information System.

8. Three data protection officer exams were organized.

9. Ensured verification of data protection officers qualifications and the extension of their qualifications.

10. 955 supervisory inspections were carried out and 192 corrective measures were applied.

2. SCOPES OF THE INSPECTORATE'S ACTIVITIES

2.1. INSPECTORATE'S INVOLVEMENT IN THE IMPLEMENTATION OF THE DATA REGULATION

The quality of national laws and regulations and policy documents and compliance with the basic principles of personal data processing is an essential prerequisite for the processing of personal data to be legal, for controllers and data subjects to be able to understand their rights and obligations, and for the Inspectorate to be able to perform effective supervision over the processing of personal data. Thus, the Inspectorate has determined participation in the creation of an orderly legal environment as one of its tasks.

For the successful completion of the mentioned task, on August 15, 2023, the Cabinet Regulations No. 448 "Amendments to the Cabinet Regulations No. 606 "Rules of Procedures of the Cabinet" adopted September 7, 2021" were adopted, designating the Inspectorate as the institution whose opinion is required in the process of coordinating a draft law or regulation, or a draft policy planning document, if the project being coordinated involves issues of personal data processing, including the processing of personal data in information systems.

In total, in 2023, 119 draft legal acts were received for coordination in the TAP portal. A total of 274 opinions were provided for these projects (of which 119 were initial opinions and 155 were repeated opinions).

In addition to the aforementioned, during the reporting period, the Inspectorate, in accordance with the sub-clause 5.6 of the Cabinet Regulation No. 368 "Procedure for Supervising the Development and Liquidation Activities of Information Systems and the Necessary Information and Communication Technology Resources and Services" adopted July 4, 2023, provided 25 opinions to the controllers on their developed descriptions of development activities for state information systems in which data processing is carried out.

During the reporting period, the Inspectorate was involved in providing opinions on the draft legal act "Amendment to the Punishment Register Law"[2]. The draft legislation was developed, among other things, taking into account the findings expressed in the Constitutional Court's judgment of December 22, 2022, in case No. 2022-09-01. Consequently, the Constitutional Court recognized Clause 1 of Section 23 of the Punishment Register Law, insofar as it relates to information about acquitted persons, as inconsistent with Section 96 of the

[2] Draft Legislation No. 23-TA-615

Constitution of the Republic of Latvia and not in force from July 1, 2023. Although the Inspectorate did not object to the amendment, which will no longer store information about acquitted persons in the Punishment Register archive database, as this is in accordance with the findings of the Constitutional Court, at the same time, the Inspectorate drew attention to the fact that the compliance of Clause 1 of Section 23 of the Punishment Register Law with laws and regulations governing personal data processing needs to be assessed as a whole, not only in relation to acquitted persons. The Constitutional Court has also pointed this out, expressing conclusions that relate not only to the storage of information about acquitted persons in the archive database, but also to the essence and purpose of the archive, data processing for archive needs, as well as the proportionality of the specified storage period in the archive database. The fact that the court's conclusions apply not only to the storage of information about acquitted persons in the archive database, but also to the entirety of Section 23, Paragraph 1 of the Punishment Register Law, is evidenced by the Constitutional Court's analysis of the storage period in the context of the purpose of archiving, as well as the aspect that the same storage period is set for all information stored in the archive database, not just for acquitted persons.

In view of the above, the Inspectorate, giving an opinion on the draft legal act, indicated that the data retention period specified in Clause 1 of Section 23 of the Punishment Register Law should be reviewed in order to comply with the Police Directive and the Law "On the Processing of Data of Natural Persons in Criminal Proceedings and Administrative Offense Process". The Inspectorate also called for determining the purposes of data processing for which personal data will be processed, taking into account Clause 2 of Article 8 of the Police Directive, that the laws of the Member States regulating processing within the scope of this Directive specify at least the purposes of processing, the personal data to be processed and the processing intentions. Meanwhile, the purpose of the law included in Section 1 of the Punishment Register Law cannot also serve for data processing for archiving purposes, as data processing for the initial purposes set out in this Section and data processing for archiving purposes are different data processing activities with different purposes. Despite the Inspectorate's objections to the draft legislation, it was adopted by the Saeima and has already entered into force[3] .

The Inspectorate also provided an opinion on the draft law "State Defense Service Law".[4] Considering that a substantial amount of information is processed to assess the suitability of individuals for the national defense service, which also includes the processing of

[3] https://likumi.lv/ta/id/349764-grozijumi-sodu-registra-likuma
[4] Draft Legislation No. 22-TA-2481

special category personal data, such as information about a person's health status and religious beliefs, it was particularly important to establish regulations that would prevent the processing of personal data for other purposes and would not create a risk of misuse of personal data. It was also crucial to carefully analyze each type of data, ensuring that each one is truly necessary to assess a person's suitability for the state defense service. In addition, the Inspectorate was also involved in discussions about the system in which data is processed, compliance with security and organizational requirements.

The Inspectorate was also asked to provide an opinion on the proposed amendments to the Lottery and Gambling Law. The legal norms included in the mentioned draft law were intended for player profiling with the aim of identifying players at risk of addiction. To achieve the goal, it was planned to process detailed data about the player from the first time they played – frequency of visits, frequency and amount of winnings, funds spent, behavioral signs indicating a risk of addiction. Although the Inspectorate believed that the purpose was of public importance, it nevertheless expressed the opinion that such processing is permissible only in circumstances where, upon establishing the risk of gambling addiction, the gambling organizer would be obliged to take some actions to manage this risk, for example, a ban on the person continue to participate in the game. Taking into account the fact that such an obligation was not intended for gambling organizers, and in the opinion of the Inspectorate, the assessment of the risks of addiction cannot be an end in itself, the Inspectorate expressed objections to the processing of data provided for in the draft law.

2.2. MONITORING AND INSPECTIONS OF PERSONAL DATA PROCESSING

2.2.1. PREVENTIVE AUDIT ON COMPLIANCE WITH DATA REGULATION REQUIREMENTS IN STATE AND MUNICIPAL INSTITUTIONS IN RELATION TO THE POSITION OF DATA PROTECTION OFFICER

In December 2022, the Inspectorate started and in 2023 completed preventive inspection in 129 state and local government institutions[5]. The audit focused on the evaluation of compliance with specific aspects, namely, whether the requirements for the appointment and notification of data protection officers to the Inspectorate are observed, and whether the conditions for the performance of the duties of the data protection officer in accordance with the Data Regulation requirements are met.

During the inspection, the Inspectorate did not identify any significant non-compliance with the Data Regulation requirements. It has also been concluded that 83 of the appointed data protection officers are included in the list of data protection officers maintained by the Inspectorate. Meanwhile, those specialists who are not included in the aforementioned list have been appointed from the internal resources of the institutions. To ensure appropriate qualification and knowledge level, these institutions regularly assign its specialists to training.

Overall, the involvement of the data protection officers in internal processes is increasing and their opinion is being taken into account, which in turn indicates that the position of the data protection officers in institutions is strengthening as a significant tool in the implementation of data protection requirements. However, there are still plenty of situations where institutions do not involve a data protection officer in the creation of their internal processes and the development of new legislative projects, which can lead to the created services/processes not complying with the requirements of the Data Regulation. It was also found that, in cases where one data protection officer performs duties in several institutions, unified document forms are often used, which are similar in content, without evaluating the specifics and functions of each particular institution.

[5] https://www.dvi.gov.lv/lv/jaunums/pern-veiktas-vairak-neka-100-preventivas-parbaudes-valsts-un-pasvaldibas-iestades

2.2.2. PREVENTIVE AUDIT IN THE FIELD OF TELEMARKETING

Continuing the initiative started in 2022 and taking into account the information obtained from processors during the 2022 preventive telemarketing check, on-site inspections were carried out at 10 controllers whose type of activity is related to telemarketing, including the operation of outbound call centers. It is essential to note that the primary aim of these inspections was not to punish controllers for non-compliance, but rather to understand the field and average practices in the industry from the Inspectorate's perspective.

The object and purpose of the on-site inspection was to assess the compliance of data processing for telemarketing purposes carried out by the data controllers with the requirements of the Data Regulation, including the principle of accountability, the implementation of data subject rights and technical and organizational requirements, as well as to check the compliance of activities with the requirements of the Law on Information Society Services.

The selection of the 10 (out of 22) companies included in the audit was carried out according to the following criteria and procedures:

1) an active client or former client to a telemarketing service provider during the period from January 1, 2022 to mid-April 2023, whose type of activity is related to telemarketing, including outbound call center operations, and who as a processor was audited in 2022 within the framework of preventive checks in the field of telemarketing in relation to processors;

2) an active company, registered in the Republic of Latvia. Operates in the Republic of Latvia;

3) it is considered that the target audience for the company's telemarketing activities are natural persons;

4) controllers were selected, with whom the Inspectorate has not carried out any initiative, preventive or other types of checks in the last two years (2021 and 2022);

5) from the remaining companies, the controllers with the lowest financial turnover in 2021 were selected, additionally noting that in the spring of 2023, the Inspectorate implemented a social campaign addressed specifically to small and medium-sized enterprises (data obtained from the database of the Register of Companies (period from 01.01.2021. to 31.12.2021.)).

As a result, 10 controllers were selected. However, noting that two of the controllers provided information that telemarketing services were not received from the specific processors during the period from January 1, 2022 to April 2023, these controllers were excluded from the

preventive inspection, and thus, upon re-application, including the criterion of the lowest financial turnover in 2021, two other controllers were selected.

The inspections consisted of two parts: a question-and-answer session where all 10 controllers were asked the same questions about their practices in the sector regarding compliance with the Data Regulation and the Law on Information Society Services, with a strong focus on the implementation of technical and organisational requirements, and a demonstration session where the controllers showed the functioning of their systems for processing customer personal data.

Following the inspection, a report was prepared with the main conclusions from the information obtained during the inspection and deficiencies in the supervisory activities related to data processing within the framework of telemarketing and sending of commercial notifications.

From the information obtained during the inspection, it was concluded that the least improvements are needed in relation to the training of employees in charge of working with personal (client) data, on the other hand, the most common deficiencies and shortcomings were observed in the drafting of contracts between the controller and the processor, where contracts are often prepared according to the principles and templates of universal contract creation, without including information specified in the Data Regulation. Improvements are also needed in the formulation and acquisition of consent to receive calls, as well as in determining data deletion deadlines and information encryption. Possible discrepancies were also identified, for example, using automatic phone number generation, establishing an appropriate legal basis, ensuring personal data integrity. Similarly, in practice, companies do not have a unified understanding of exactly when an offer made during a call would or would not be considered a commercial announcement in the context of the Law on Information Society Services.

Overall, the potential non-compliances are not associated with significant restrictions on the rights of data subjects, grossly violating the Data Regulation, as well as the requirements of the Law on Information Society Services; however, the results of the audit took into account the recommendations of the supervisors on the need for advisory explanations, for example, on the type and duration of data storage. As a result of the inspection, it was also concluded that, like after the telemarketing inspection at the processors, guidelines or recommendations useful for the controllers need to be prepared after this inspection, in order to standardize practice and operate in accordance with the Data Regulation and the Law on Information Society Services.

As a result of the audit, guidelines "Processing of Personal Data in the Field of Telemarketing as a Processor" were developed, which are available at:

https://www.dvi.gov.lv/lv/dvi#personas-datu-apstrade-telemarketinga-joma-apstradataja-statusa

2.2.3. SUPERVISION OF DATA PROCESSING

During the reporting year, the Inspectorate received 789 complaints from data subjects about possible personal data processing violations, 78 notification reports about personal data protection violations, and 88 submissions from other third parties (public institutions, organizations, associations) about possible personal data processing violations. Based on the received complaints, notifications of personal data protection violations, and the initiative of the Inspectorate itself, the Inspectorate conducted a total of 955 checks on personal data processing (including initiative checks) within the framework of the administrative process and administrative offense process throughout the year.

The slight increase in the number of reviewed inspection cases compared to the previous reporting period can be explained by the fact that citizens become more and more attentive and cautious about the security of their data. At the same time, the Inspectorate has observed that the received complaints often contain information about systematic violations by the controller, affecting a wider range of data subjects.

Areas where inspections were carried out:

1) personal data processing on online social networks and other internet sites;

2) conducting video surveillance in public places, private properties, businesses and institutions;

3) personal data processing in state institution information systems;

4) respecting the rights of data subjects;

5) personal data processing in the process of extrajudicial debt recovery and personal credit history evaluation process;

6) processing of children's personal data;

7) processing of special category personal data (including health data);

8) personal data processing in e-commerce, commercial notification sending, and telecommunications;

9) personal data processing carried out by mass media;

10) personal data processing using cookies.

2.2.3.1. NUMBER OF RECEIVED COMPLAINTS

The largest number of complaints – 226 out of 789 received complaints – during the reporting period were submitted about the processing of personal data in online social networks and other internet sites. In most cases, personal data processing was not identified, but a potential privacy infringement or violation of website usage rules was detected. Therefore, data subjects were informed about their rights to approach the website administrator with a relevant request. During the reporting period, there has been an increase in the number of complaints where the data subject's information, which is published on social networks or forwarded in private correspondence, is used for fraudulent purposes, creating fake profiles on social networks. Compared to the previous year, it is still observed that individuals, in case of doubts about unlawful data processing, do not use the mechanism provided by the Data Regulation for the protection of their rights, by addressing the data processing controller, and also do not use the possibilities provided on social network platforms to request the deletion of information, but instead immediately turn to the Inspectorate.

The second area where complaints were most frequently received was video surveillance. Considering that the technical capabilities of surveillance cameras are continuously being improved and the devices are available to a wide range of citizens, there is a trend that surveillance cameras are widely used, without the public knowing or being aware of the basic principles of video surveillance. Upon examining such complaints, similar to previous reporting periods, it was found that most often there are no informational signs about video surveillance, or the informational sign does not contain all the necessary information specified in the paragraph three of Section 36 of the Data Law (the name of the controller, contact information, purpose of data processing, as well as a reference to the possibility of obtaining other information indicated in Section 13 of the Data Regulation). It has also been observed that data controllers often do not want to install an informational sign, believing that their rights are being violated, as the information becomes publicly available.

During inspection of conducted video surveillance, it has been observed that data controllers, when defining the purpose of personal data processing, often indicate that video surveillance is carried out to ensure public order, thereby attempting to stop (in the controller's view) the illegal activities carried out by a neighbor and assuming the functions of law enforcement agencies. In addition, a trend was observed during the reporting period that the number of complaints about the use of smart devices equipped with video recording function (for example, smart doorbells) is also increasing.

Compared to 2022, the number of complaints about personal data processing in state institution information systems has decreased – a total of 67 complaints were received and examined in this area. At the same time, it has been noted that citizens are increasingly complaining about the actions of various medical personnel, checking personal data in the unified health system (E-Health) without any legally justified reason, namely, personal data has not been reviewed within the framework of a medical episode.

In 2023, while the Inspectorate examined the complaints of data subjects, it applied corrective measures (warning, order, reprimand, processing restriction) in 192 cases, calling on controllers to fulfill the controller's duties specified in the Data Regulation. Among them, the controllers were obliged to comply with the data subject's request, to implement appropriate technical and organizational measures to ensure and be able to clearly demonstrate that the processing is in accordance with the requirements of the Data Regulation, to coordinate the personal data processing activities carried out with the provisions of the Data Regulation regarding the correction or deletion of personal data, or restriction of processing.

2.2.3.2. REPORTING THE PERSONAL DATA PROTECTION VIOLATIONS

In the event of a personal data protection breach, in accordance with Article 33(1) of the Data Regulation, the controller has an obligation to report the breach of personal data protection to the Inspectorate without undue delay and, if possible, not later than 72 hours from the moment when the breach became known to him or her, except in cases where it is unlikely that the personal data protection breach could pose a risk to the rights and freedoms of natural persons. In 2023, the Inspectorate received 78 reports of personal data protection violations, of which 74 reports contained information about confidentiality violations, 4 – about integrity, 4 – about accessibility violations.

During the reporting period, the Inspectorate received several personal data protection violation reports, which contained information about unlawful acquisition and publication of personal data in commercial locations. Thus, security personnel at the trading venues filmed surveillance camera records on their personal smart devices and published them on various social networks.

2.2.3.3. DECISIONS MADE IN ADMINISTRATIVE OFFENSE CASES

During the reporting period, the Inspectorate made 9 decisions in administrative violation cases, in all cases imposing a fine on the offender.

In cases of administrative violations, the range of fines applied in the reporting year ranged from 300 *euros* to 20,000 *euros*. In 2023, the Inspectorate applied fines in the total amount of 26,500 *euros*.

All the mentioned penalties were applied for violations for which responsibility is provided in the relevant sub-clause of Article 83(5) of the Data Regulation.

In two cases, penalties were imposed for violation of the data subject's rights in accordance with Articles 12-22 of the Data Regulation (sub-clause a) and b) of Article 83(5) of the Data Regulation).

In one case – for non-compliance with the supervisory authority's order or data flow restriction in accordance with Article 58(2) of the Data Regulation, or for not providing access, violating Article 58(1) of the Data Regulation (sub-clauses a), b) and e) of Article 83(5) of the Data Regulation).

In one case, for the controller's actions by not providing the Inspectorate with the information it requested, which is necessary for the performance of the Inspectorate's tasks (Article 83(5)(e) of the Data Regulation).

In five cases, penalties were imposed based on the paragraph four of Section 3 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 false information to the Inspectorate).

2.3. CONTESTING AND APPEALING DECISIONS MADE BY INSPECTORATE'S OFFICIALS

2.3.1. CONTESTATION

The Director of the Inspectorate has made a total of 12 decisions in 2023. In the cases of administrative offense process, three decisions made by officials have been appealed, while in the cases of administrative process, eight decisions made by officials have been contested. One decision has been made to leave the complaint in the administrative violation case without progress.

Regarding the appealed administrative violation cases, it should be noted that in all three cases, the Director's decisions were made to leave the appealed decision unchanged.

At the same time, regarding the administrative proceedings appealed to the Director, it should be noted that six decisions have been made to recognize the actual action as legal, but two decisions have been made to recognize the actual action as illegal and the case materials have been handed over to the relevant Inspectorate department for reconsideration.

2.3.2. PROCEEDINGS

In total, 8 final court decisions were adopted during the reporting year. Of these, two decisions are in administrative violation cases, and six are in administrative process cases.

All the mentioned court decisions are favorable to the Inspectorate.

One of the most interesting administrative process cases that concluded during the reporting period was the case regarding video surveillance conducted by the Bank of Latvia within the framework of ensuring national security. Accordingly, an individual had approached the Inspectorate with a complaint about the video surveillance of an individual in the area adjacent to the Bank of Latvia building, believing that the Bank of Latvia had carried out the aforementioned processing in violation of the Data Regulation requirements.

Upon evaluating the aforementioned complaint, the Inspectorate determined that the building of the Bank of Latvia is a state-protected object around which a 25-meter wide protective zone has been established, and at the same time, this building is also a critical infrastructure object. Considering the above, it was recognized that the video surveillance of the building of the Bank of Latvia and its adjacent territory is a measure taken to ensure the physical security of this building as a state defense object and critical national infrastructure, namely, it is an activity related to ensuring national security and it does not fall within the scope of the Data Regulation and is not within the competence of the Inspectorate.

The natural person appealed the decision of the Director of Inspectorate to the court, where with the judgment of the Administrative District Court[6] it was recognized that the decision of the Director of the Inspectorate is legal, while the application of a natural person can be rejected. The Administrative Regional Court, upon reviewing the appeal complaint of the individual, concluded that the individual's appeal complaint is unfounded and that the application should be dismissed.

As part of the examination of the mentioned case, the court recognized:

[6] Legal proceedings case No. A420283521

- Article 2(2)(a) of the Data Regulation, read in the light of Recital 16 of the Data Regulation, can be considered as having the sole purpose of excluding from the scope of the Data Regulation the processing of personal data carried out by public authorities within the scope of an activity aimed at protection of national security, or as part of an activity that can be included in the same category;
- as the processing of personal data carried out by the Bank of Latvia falls under the exception mentioned in Article 2(2)(a) of the Data Regulation, when the Data Regulation is not applied, the Inspectorate has duly considered the complaint in accordance with Article 57(1)(f) of the Data Regulation and found that it is not within the competence of the Inspectorate to assess the substance of the individual's complaint;
- the court disagrees with the individual's opinion that the three-month term applies to the overall consideration of the case in the institution. As mentioned, Article 78 of the Data Regulation stipulates that the supervisory authority must examine the data subject's complaint within three months and inform about its progress or results. The Inspectorate has done that. It is up to the individual to decide whether to challenge this response.

It is also worth mentioning an administrative offence case in which the processing of personal data by SIA "Tet" was found not to comply with the requirements of the Data Regulation. The technical solutions implemented by the company allowed the possibility for a client to apply for the Tet+ service on the website without confirming the contract, using another person's personal identity number, without verifying the identity of the service recipient. As a result, when preparing and posting the contract in the customer self-service system *Mans Tet,* the data of the owner of the personal identity number was disclosed to third parties.

SIA "Tet" contested the initial decision by which an administrative fine of 3.2 million *euros* was applied to the Director of the Inspectorate, who made a decision to amend the amount of the penalty, applying an administrative fine of 1a2 million euros to SIA "Tet" for the violations found. The amount of the fine was reduced by re-evaluating criteria such as the number of data subjects affected, the level of responsibility of the controller or processor, taking into account the technical and organizational measures implemented. It was also taken into account that data processing is only a part of the core activities of SIA "Tet".

The company appealed against the Inspectorate Director's decision in court. With the judgment of the court of first instance[7] it was decided to leave the Inspectorate's decision

[7] Legal proceedings case No. 01630000100222.1.

unchanged, and to reject the complaint of SIA "Tet". The examination of the case in the appellate instance continues even after the specific reporting period.

2.4. CASE STUDY

2.4.1. ON VIDEO SURVEILLANCE CONDUCTED BY THE EMPLOYER AT THE WORKPLACE

The Inspectorate received information indicating that the employer (a state administration institution) is processing personal data through video surveillance, including observing employee desks and monitors, as well as serving clients. The information available to the Inspectorate also indicated that the video equipment installed in the workspaces could also make audio recordings.

The employer justified the processing of personal data in the form of video surveillance based on Article 6(1)€ of the Data Regulation, in order to reduce the risk of corruption and ensure fact-checking if information about a possible violation was received. The possibility was also not excluded that the data obtained as a result of video surveillance would be used for another, undefined purpose, namely, detecting a criminal offense against property.

The Inspectorate concluded that video surveillance in the workspaces was installed following the discovery of a corruption case; however, prior to the implementation of video surveillance, no assessment was made on the impact of whether the data obtained as a result of video surveillance could significantly reduce corruption risks. In addition, the consideration that visitors may come to the employees of the institution at any time and in the event of their non-observance there is a risk of bribery and the risk of making an illegal decision is not a sufficient justification for the conducted data processing to be proportionate. Essentially, knowing about video surveillance, corrupt activities can be carried out outside the office. The Inspectorate concluded that there are no laws and regulations in the field of corruption prevention that directly provide or contain a general regulation on the need for video surveillance in the premises of state institutions. At the same time, the invasion of personal privacy caused by video surveillance in the workplace, observing them throughout the working hours, is significantly greater than the result obtained; therefore, the respective purpose – reducing the risk of corruption – can be achieved with other measures and activities that do not involve personal data processing at all or to a lesser extent.

In light of the above, the Inspectorate concluded that video surveillance in the workplace cannot be carried out in this particular situation, and the controller (employer) was subjected to corrective action – a warning, as well as an obligation to stop video surveillance in the workplace and delete the data obtained as a result of video surveillance.

2.4.2. STORAGE OF PERSONAL IDENTIFICATION DOCUMENTS ON WORK COMPUTERS

The Inspectorate received information indicating that copies of personal identification documents were being stored in an unprotected manner on work computers in several stores of one company.

During the inspection, it was found that the company, while selling goods, offers the services of a cooperation partner and the option to purchase goods on installment. For a client to arrange a deferred payment purchase, they must present a document confirming their identity, a copy of which the company later delivers to the cooperation partner. Thus, it was determined that the company, by obtaining and transferring a copy of a person's identification document, acts on behalf of a cooperation partner and is considered a processor in the understanding of the Data Regulation.

During the inspection, it was found that copies of personal identification documents, after being sent to a cooperation partner, were stored on the work computer for an unlimited period of time and they were accessible to all employees of the specific store, as multiple users were not set up on the computers.

In addition, it was found that employees were not instructed that after processing client’s personal data, document copies must be deleted from the computer.

Noting that the company processed (stored) personal data after the task of personal data processing had been completed, it was established that the company becomes an independent personal data controller after achieving the goal of personal data processing set by the controller, thus such data processing must comply with the requirements of the Data Regulation, including the legal basis for personal data processing.

During the inspection, the company was obliged to cease the processing of personal identification documents without legal basis and to delete copies of personal identification documents stored in the store's computers.

2.4.3. PROCESSING OF PERSONAL DATA WITHOUT CONSENT

The Inspectorate received information that the controller is processing personal data of individuals (clients/data subjects) without an appropriate legal basis and contrary to the basic principles of data processing set out in the Data Regulation.

The controller, who is engaged in taking photographs and selling the obtained photographs to data subjects, has stipulated in the Personal Data Processing Rules that all clients are issued an item, which, depending on its color, indicates whether the person wants or does not want the photographer to freely photograph the person. If a person wishes to be photographed, they can approach the controller after some time and purchase the photographs in which they are visible.

The inspection found that in practice the Personal Data Processing Rules regarding the issue of the subject do not work, as they are not issued to the customers, and the photographer takes pictures of any person who apparently expresses a desire to be photographed, for example, looks at the photographer or smiles.

The Inspectorate concluded that the controller has been and continues to process personal data of data subjects (photo acquisition, storage), based on a legal basis that does not comply with the requirements of the Data Regulation for obtaining valid consent. The Inspectorate also concluded that the controller has provided data subjects with general information about personal data processing but has not taken appropriate measures to fully implement the rights of data subjects in accordance with the requirements of Article 12(1) of the Data Regulation, i.e., has not ensured the fulfillment of the obligation to provide clear, understandable and precise information to data subjects regarding data processing. For the committed violations, the Inspectorate imposed a fine of 1,000 *euros* on the controller.

2.4.4. TRANSFER OF PERSONAL DATA OF OTHER INDIVIDUALS

During the reporting period, the Inspectorate completed an audit in a case where another person's data had been incorrectly provided.

In this particular case, the institution approached the state information maintainer, requesting information about a specific individual, indicating this person's name, surname, and erroneously specifying another person's personal identity number. The respondent, in providing the answer, has indicated the name and surname of the person for whom the information was

requested; however, the information provided was about the owner of the incorrectly specified personal identity number.

During the inspection, the Inspectorate found that the state information system maintainer, when providing information about individuals in its database, has defined only the personal identity number as a selection criterion, believing that the search criterion – name and surname – would exceed the principle of minimization; moreover, the person's name and surname are not visible even when the record of the respective personal identity number's owner is found.

The Inspectorate concluded that if individuals could be located in the information system by their first and last names, it would not exceed the principle of minimization, but rather ensure that information is provided about the requested person, not the owner of the erroneously indicated personal identity number.

During the inspection, the Inspectorate imposed an obligation on the state information system maintainer to improve the practice of fulfilling institutional requests.

2.4.5. PERSONAL DATA PROCESSING (PUBLICATION) IN THE PUBLIC REGISTER

In 2023, the Inspectorate reviewed a case regarding the publication of personal data in a public register, which includes information about the trademark owner: name or first name, surname, and their address.

National regulations provided for the publication of only the name, first name and surname, but did not provide for the publication of the natural person's address. The purpose of publication is to provide information about the trademark owner, so that a person who wishes to use the trademark and needs to contact the trademark owner, would have the opportunity to communicate with them.

Upon evaluating the overall situation, the Inspectorate recognized that the publication of the relevant personal data can be justified under Article 6(1)(e) of the Data Regulation and the data of the trademark owner can be processed to ensure the rights of the trademark owner to manage the use of the trademark, as well as to ensure the implementation of the rights of other persons and the requirements of laws and regulations in the field of intellectual property protection. However, considering that the law stipulates data to be published in a comprehensive manner, not allowing additional data publication, the Inspectorate urged the controller to initiate amendments to the laws and regulations to ensure lawful processing of personal data.

.

2.4.6. VIEWING PERSONAL DATA IN THE NATIONAL INFORMATION SYSTEM

During the reporting period, the Inspectorate examined a case regarding personal data processing in the E-health system. An individual, while checking the audit records available in E-health, found that information about the person was accessed more than 30 times by a medical professional who did not prescribe medication to the data subject, issue sick leave, or make other changes to the patient's record.

During the inspection, it was found that an employee of the medical institution viewed personal data without a legal basis. At the same time, it was found that the rules for compliance with data protection requirements are included in the job description, which employees sign together with the employment contract when starting employment relations; however, training on personal data processing only took place after the initiation of the Inspectorate's audit.

Taking into account all the circumstances of the case, the Inspectorate applied a corrective measure and issued a warning to the medical person.

2.4.7. PROCESSING OF PERSONAL DATA ON THE WEBSITE USING COOKIES WITHOUT APPROPRIATE LEGAL BASIS

During the reporting period, the Inspectorate completed an investigation into a case where personal data processing violations were found on a website using cookies without an appropriate legal basis, and applied a corrective measure – fine.

During a preventive inspection of several company websites, the Inspectorate found discrepancies in several of them in relation to the legal use of cookies, which did not comply with the requirements of the Data Regulation and Law on Information Society Services Law. Accordingly, the Inspectorate invited the controllers (companies) to review and rectify the identified deficiencies, as well as to provide a response about the measures taken.

Considering that in this particular case the controller had not provided a response within the set deadline, the Inspectorate repeatedly addressed the controller and, upon the controller's request, extended the deadline for compliance with the invitation. However, during subsequent inspections, it was found that the identified deficiencies were not corrected, including the fact that analytical cookies were set on the website before receiving the user's informed consent.

Overall, during the repeated inspections within the scope of the audit case, it was concluded that the website still did not provide comprehensive, clear and understandable information to the user about the types of cookies used and their purposes, and several cookies were used without an appropriate legal basis. Considering the fact that, despite the repeated calls of the Inspectorate and the provided explanations of the legal framework, there were still significant deficiencies on the website, the Inspectorate found the company guilty of the identified violations of personal data processing and imposed a fine of 20,000 *euros* on the controller.

2.5. INTERNATIONAL COOPERATION

2.5.1. ENSURING CONSISTENCY

In 2023, the Inspectorate continued its active involvement in the development of EDPB working documents. The Inspectorate, as the leading reporter, has begun work on preparing guidelines for the use of supervision lists in the field of prevention of money laundering. The Inspectorate has also been involved as a co-reporter in the development of guidelines related to the implementation of the Digital Market Law. Work has been completed on the preparation of the EDPB opinion on the approval of accreditation criteria for the Romanian supervisory authority's code of conduct, where Latvia was the main reporter, and work has also been completed on the certification criteria of the Maltese certification authority, where the Inspectorate acted as a co-reporter. The accreditation criteria for the Latvian Code of Conduct Supervisory Authority have been approved.

The Inspectorate has also participated in the preparation of other EDPB documents as a commentator and proposer of suggestions.

Particularly noteworthy is the Inspectorate's activity in the second coordinated EDPB implemented audit. Throughout the year, 26 supervisory authorities across the European Economic Area (EEA), including the Inspectorate, carried out a coordinated supervisory measure to assess the appointment and performance of data protection officers.

To assess whether the position of a data protection officer in the institutions of the Republic of Latvia complies with the conditions of the Data Regulation, as well as to identify the necessary resources for the performance of the data protection officer’s duties, the Inspectorate sent survey questionnaires prepared by EDPB to the ministries and their subordinate institutions. During the inspection, 179 responses were received from the institutions. In almost all of the mentioned institutions, a data protection officer has been

appointed to help ensure the processing of personal data in accordance with laws and regulations. Considering that in the modern era of digitalization, data security risks are increasing, it is clear that the position of a data protection officer in institutions is essential and necessary. More information is available at: https://www.dvi.gov.lv/lv/jaunums/noslegusies-parbaude-par-datu-aizsardzibas-specialista-institutu. Meanwhile, we invite you to familiarize yourselves with the report: https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en

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

In addition to the tasks set out in the Data Regulation and in accordance with special laws and regulations, the Inspectorate has a duty to monitor the processing of personal data in large-scale IT systems of the European Union.

For the effective supervision of personal data processing, the Inspectorate must handle complaints, conduct regular audits, and carry out other supervisory activities that would promote a more effective protection of personal data in the SIS II, VIS and Eurodac systems.

During the 2023 period, preparations continued for the supervision of compliance with personal data protection requirements in large-scale IT systems, the operation of which is planned to start in the near future – ECRIS, ETIAS and Satvara – which ensure the mutual usability of the data accumulated and processed in these information systems.

The implementation of the system has been postponed several times, as the initiation of the main system operation is delayed. Consequently, the Inspectorate's planned supervision measures are also accordingly distanced.

At the same time, the monitoring of currently operational systems is being implemented with increasing quality, diversifying the monitoring measures taken and, along with the growth of the Inspectorate's institutional experience, also making the actions taken more effective.

2.5.3. SCHENGEN INFORMATION SYSTEM

In 2023, an inspection was carried out on the compliance of alert placement in the system with the conditions of [8] chapter VII of the SIS II decision. Based on the audit findings,

[8] Regulation No. 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/TI and repealing Regulation (EC) No.1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

it was expanded to also evaluate end-user data operations at the police station. During the inspection, no inconsistencies were found regarding the procedure for creating and placing warnings in the system.

A regular inspection was carried out on the compliance of the standard response data subjects used by the SIRENE office with laws and regulationsgoverning SIS II operations. During the inspection, copies of the used sample responses were received, and their compliance analysis was carried out.

Within the framework of supervisory measures, the Inspectorate, in cooperation with representatives of the State Police, has developed a training program for the use of the N.SIS by State Police employees. The training course was utilized within the framework of the State Police College training programs.

In the upcoming reporting period, the Inspectorate plans to continue the initiated cooperation in relation to enhancing the knowledge and skills of the State Police personnel regarding personal data protection.

2.5.4. VISA INFORMATION SYSTEM

In 2023, an audit was conducted on information processing at one of the N.VIS connection points – the Latvian Embassy in Kazakhstan. Based on the findings during the inspection, the scope of the inspection was expanded and the inspection related to N. VIS issues was also carried out in the central apparatus of the Ministry of Foreign Affairs. During the inspection, no significant discrepancies were found in relation to the logical and physical security requirements of the system operation. Based on the findings, the development of proposals for measures necessary for a more efficient operating mode of the system continues.

During 2023, a plan for the elimination of inconsistencies found during the audit of OCMA was coordinated. Measures have been initiated to carry out the implementation control of the plan.

2.5.5. EUROPEAN ASYLUM SEEKERS FINGERPRINT DATABASE (EURODAC)

Within the framework of the 2023 supervision measures, the Inspectorate checked how the respective institutions are addressing the discrepancies identified in the previous audit report and implementing the recommended improvements. No deviations from the agreed supplement implementation plan were found during the supervision measures.

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

At the end of 2021, the Inspectorate submitted a project proposal to the personal data protection supervisory authorities in tender No. CERV-2021-DATA announced within the framework of the European Commission's financial program "Citizens, Equality, Rights and Values" (CERV) for 2021-2027, in order to increase the knowledge of target groups' level on data protection regulations and their implementation. In March 2022, the European Commission approved the project proposal submitted by the Inspectorate for its implementation. On September 1, 2022, the Inspectorate signed an agreement with the European Commission on the implementation of the project. The project aims to develop a distance learning program in personal data protection for representatives of small and medium-sized enterprises, thereby creating a free tool for this target group to acquire knowledge and practical skills in the field of personal data protection and to use the acquired knowledge in their companies. The training is designed to provide both theoretical knowledge and practical tasks. The training program will be available not only in Latvian, but also in English and Russian. On July 21, 2023, a contract was concluded with SIA "Datorzinības centrs" for the "Development, localization, and technical provision of the content and interactivity of the E-learning "Personal Data Protection for Small and Medium Enterprises" (procurement identification No. DVI 2023/2). Information about the project is available on the Inspectorate's website. It is planned that the distance learning program will be available for learners in 2024.

2.6. INSTITUTE OF A DATA PROTECTION OFFICER

The Data Protection Officer is a person who has professional qualifications, especially special knowledge in the field of data protection rights and practices, and the ability to perform the tasks mentioned in Article 39 of the Data Regulation. The duties of a data protection officer can be performed both by a person who has passed the qualification exam organized by the Inspectorate (included in the list of data protection officers[9]), and by a person who has not taken or passed such an exam, but who has sufficient theoretical and practical knowledge in the field of data protection.

The second half of 2023 was marked by the maintenance of the data protection offiers' qualifications. In accordance with Paragraph 54 of the Cabinet Regulation No. 620 "Regulations Regarding the Qualification of a Data Protection Officer" adopted on October 6,

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

2020; in 2023, the qualification maintenance period had begun for the majority of individuals included in the list of data protection officers. These individuals were included in the list before the aforementioned regulations came into force, thus the qualification maintenance period, during which to attend or lead qualification maintenance events, was three years from the day the regulations came into force and will commence in the fall of 2023. Individuals included in the list of data protection officers were sent reminders in a timely manner about the approaching application submission deadline and the actions to be taken for successful maintenance of qualifications. This information was also published on the Inspectorate's website.

245 data protection officers submitted applications for maintaining their qualification. Upon evaluation of the submitted applications, two decisions were made to exclude individuals from the list of data protection officers, 11 decisions on partial recognition of data protection officer's qualification maintenance[10] and 232 decisions on recognition of data protection officer's qualification maintenance. Two applications were also received from individuals who were not included in the list of data protection officers.

By the set deadline (08.12.2023), applications for maintaining the qualification of a data protection officer have not been submitted, and thus 93 persons have been excluded from the list of data protection officers.

In 2023, in accordance with Clause 4 of Paragraph one of Section 4 of the Data Law, 3 data protection officer qualification exams were organized, in which 64 candidates participated, of which 50% or 32 successfully passed the exam and thus their information was included in the list of data protection officers published by the Inspectorate.

In 2023, a practice was initiated to send out post-examination evaluation surveys to candidates after each exam, in which candidates express their satisfaction or dissatisfaction with the practical conduct and organization of the exam, what is useful feedback for improving the quality of future exams. Overall, the organization of the exams was evaluated positively; however, feedback was received about the exam being overly complex, as well as suggestions to either extend or shorten the exams. However, a large part of the objections are not feasible, considering that this knowledge test is primarily organized in accordance with the guidelines

[10] In accordance with Paragraph 50.3 of the Cabinet Regulation No. 620 "Regulations Regarding the Qualification of a Data Protection Officer" adopted on October 6, 2020, the Inspectorate within one month after receiving the qualification maintenance application, makes a decision to partially recognize the training as a data protection officer qualification improvement measure and data protection officer qualification maintenance, setting an obligation for the data protection officer to participate in the training for a specified number of academic hours, if the duration of the training attended by the data protection officer is at least 18 academic hours, but less than 36 academic hours.

included in the Cabinet Regulation No. 620 "Regulations Regarding the Qualification of a Data Protection Officer" adopted on October 6, 2020.

In 2023, 38 public sector institutions and 101 private legal entities reported the appointment or replacement of 139 data protection officers. In certain cases, one controller has appointed more than one data protection officer. Of the appointed officers, in 113 cases they are included in the Inspectorate's public list of data protection officers. In accordance with Article 37(7) of the Data Regulation, it is the controller's duty to publish the contact information of the data protection officer and notify the supervisory authority, in Latvia – the Inspectorate. Information about the appointment or change of a data protection officer is also submitted to the Inspectorate by companies that are not registered in Latvia, but their clients and data subjects may be residents of Latvia.

2.7. SUPERVISION OF CREDIT BUREAU OPERATIONS

In accordance with the Law on Credit Bureaus and the Cabinet Regulations No. 267 of "Regulations Regarding Licensing and Supervision of Credit Bureaus" adopted on June 2, 2015, two credit bureaus are registered in Latvia – joint stock company "Kredītinformācijas birojs" and joint stock company "CREFO birojs". The purpose of operation as defined in the Law on Credit Bureaus is to contribute to the promotion of responsible lending and responsible and honest borrowing, promoting the formation of credit history of individuals, as well as to ensure the protection of the rights of natural persons, so that true and complete information is available and used when assessing creditworthiness. Credit bureaus are licensed and their operation is monitored by the Inspectorate. The Inspectorate, in accordance with the Paragraph one of Section 23 of the Law on Credit Bureaus and on its own initiative, carried out preventive checks on the compliance of personal data processing carried out by the credit bureau with the requirements of the Data Regulation and the Law on Credit Bureaus. In the inspection of 2023, the Inspectorate focused on the interpretation of the Paragraph one of Section 16 of the Law on Credit Bureaus, specifically, how long information about the insolvency process should be stored. The inspections were carried out on-site at the premises of AS "Kredītinformācijas birojas" and AS "CREFO birojs". Overall, within the framework of preventive inspections, significant non-compliances with the Data Regulation and the Law on Credit Bureaus were not identified in AS "CREFO birojs" and AS "Kredītinformācijas birojs".

During the reporting period, the Inspectorate provided consultations to credit bureau representatives on the application of the Law on Credit Bureaus. An assessment of the suitability of new board members was also carried out, in accordance with the procedure set out

in the Cabinet Regulations No. 267 "Regulations Regarding Licensing and Supervision of Credit Bureaus" adopted on June 2, 2015 .

2.8. COMMUNICATION WITH THE PUBLIC

In the daily work of the Inspectorate, communication with the public is significant, as with the enforcement of the Data Regulation, which began on May 25, 2018, the primary task of the Inspectorate as a supervisory authority is to promote public understanding of individual rights to privacy and the responsibility of relevant persons to ensure appropriate technical and organizational measures to ensure safe personal data processing and protection.

2.8.1. #DVISKAIDRO

.

To ensure easily accessible information for everyone on current data protection issues, the Inspectorate has been implementing an informative explanatory campaign #DVIskaidro[6] for the third year in a row. As part of it, once a week, are created explanations with recommendations on how organizations (public and private sectors) can ensure data processing in accordance with the Data Regulation, while for citizens – practical recommendations on how to exercise their rights are provided. In formulating explanations, the Inspectorate takes into account the actualities of the given moment and the questions received.

During the reporting year, the Inspectorate, in cooperation with mass media at the national and international level, ensured public information and promotion of understanding about the processing and protection of personal data in 43 cases.

2.8.2. SEMINARS

In order to provide the public with information on current data protection issues and to answer frequently asked questions, in the reporting year the Inspectorate ensured participation in 28 seminars and conferences at the national and international level, including organised online seminars on current issues in data protection:

- On January 26, marking the 17th European Data Protection Day, a seminar "Data Security and Protection in the Digital Environment" was held, informing citizens on how to ensure that their communication in the digital environment regarding their own and other people's data is safe and thoughtful;

- On May 12 – participation in the 31st International Conference "Spring Conference 2023" (Hungary);

- On May 25, marking the fifth anniversary of the Data Regulation, participation in the annual data protection and cyber security conference "Digital Era";
- On June 9, in cooperation with the Patent Office – participation in the talk festival "LAMPA" in the discussion "A frivolous date with serious consequences";

- On August 28 – Seminar for the general public on how to ensure data protection and security in the IT environment;
- On October 25 – a seminar on the most important aspects of data processing, which helps to improve the efficiency and security of data processing at your workplace;

- On December 28th – a seminar for both controllers and subjects on the use of cookies and the most frequently observed discrepancies in practice.

Continuing the practice started in 2022, cooperation with the State Employment Agency was continued during the reporting year to enhance the knowledge of persons in the status of unemployed. Eleven seminars were conducted on the topic "Data Security and Protection in the Digital Environment", where the representative of the Inspectorate explained the essence of data protection, things that every data subject should know, and also shared practical examples where individuals unknowingly harm themselves by publishing their personal data in the digital environment. The most popular myths in the field of data protection and actions to be taken to protect oneself and others from fraudsters in the digital environment were also discussed. In total, 745 clients of the State Employment Agency attended the seminars. At the end of each seminar, the audience's questions were answered, which led to a discussion of various problematic situations of the modern digital age from the point of view of the data protection and supervisory authority and citizens. The conduct and content of the seminars were positively evaluated, and words of gratitude were received from the attendees for the easy comprehensibility of the content, apt examples, and clear answers to initially unclear questions. More information available at https://www.dvi.gov.lv/lv/jaunums/inspekcija-turpina-sadarbibu-ar-nva. Considering the successful experience and interest of participants, the initiated cooperation will continue in 2024, and within its framework, 11 more lectures are planned for the clients of the State Employment Agency.

2.8.3. PUBLIC AWARENESS, RECOMMENDATIONS AND GUIDELINES

Within the framework of its basic functions, the Inspectorate carried out daily education of citizens, including foreigners, using telephone consultations, written consultations, virtual assistant Zintis available on the Inspectorate's website. The primary task of this assistant is to provide the institution's clients with answers to simple, short questions within the institution's competence. In the reporting period, 374 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 citizens, not understanding the basic function of the virtual assistant, ask long questions or describe a problematic situation, which results in an unanswered question.

In 2023, 1,956 telephone consultations, 557 written consultations and 19 face-to-face/video consultations were provided. During 2023, 563 written consultation requests were received from residents. The most frequently explained topics during consultations were

processing within the framework of employment relationships, conditions for video surveillance by physical and legal persons, video surveillance without informing data subjects, as well as observation of other private property without the owner's consent, data processing on the web and social networking sites, including cookie processing, the implementation of data subject rights in practice, and data processing carried out by the public sector. In case of problems, data subjects were explained their rights to the protection of their personal data stipulated in the Data Regulation, including turning to the Inspectorate.

Providing consultations and educating residents, including legal entities (as part of consultations and inspections) in matters of personal data processing and providing explanations contributes to the recognition of the Inspectorate in society, its reliability as a state administrative institution, as well as prevents potential violations if the controller approaches the Inspectorate with a lack of understanding about regulatory framework in the sector, the basic principles of data protection, or if the citizen is informed of his rights regarding data protection. At the same time, the "Consult First" principle is being strengthened and maintained, the implementation of which began in 2017.

Guidelines "Processing of personal data in the field of telemarketing as a processor"

To facilitate the implementation of the General Data Protection Regulation and the Law on Information Society Service, the Inspectorate has developed guidelines on the processing of personal data in the field of telemarketing. The target audience is companies whose operations are related to telemarketing, including outbound call center activities. Guidelines are available at https://www.dvi.gov.lv/lv/media/2216/download?attachment.

Developed accreditation requirements for supervisory authorities of code of conduct

In accordance with the provisions of the Data Regulation, the Inspectorate has developed and approved the accreditation requirements of the supervisory authorities of code of conduct.

Accreditation requirements for the supervisory authorities of code of conduct are available at https://www.dvi.gov.lv/lv/media/2323/download?attachment.

Meanwhile, the Cabinet Regulation No. 488 "Regulations Regarding Licensing of Supervisory Authority of Code of Conduct" adopted on August 9, 2022, determines the requirements for receiving an accreditation license, including the amount of information to be

included in the application, as well as the procedure for issuing, suspending and canceling the accreditation license, the amount of the state fee and the procedure for transferring the license.

Informative Campaign "Data is valuable – protect it!

To enhance the understanding of small and medium-sized enterprises about the importance of personal data protection and to promote the implementation of good practices in data protection, the Inspectorate carried out an informative campaign "Data is valuable – protect it!" from April 4, 2023 to June 14, 2023. Within the campaign, five seminars/workshops were also organized on the development of privacy policies in the regions – in Rēzekne, Liepāja, Jelgava, and Valmiera, as well as in Riga. A presentation has also been created to assist in the development of privacy policies.

As part of the campaign, we introduced the public to the Datiņš family.

Information about the campaign is available at - https://www.dvi.gov.lv/lv/kampana-dati-ir-vertiba-sarga-tos

Decisions, explanations and opinions of the Data State Inspectorate

To inform the public about personal data processing and protection and to promote a unified understanding of the implementation of rights and obligations set out in the Data Regulation for individuals and legal entities, the decisions made by the Inspectorate on violations of the Data Regulation requirements committed by controllers and processors, or corrective measures applied, as well as the opinions and explanations provided by the institution within its competence, are published on the Inspectorate's website during the reporting period.

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

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

3. PRIORITIES FOR THE NEXT YEAR

1. To strengthen the Inspectorate's capacity by creating a competitive and favorable work environment within the Inspectorate, attracting professional and motivated employees to ensure the execution of the Inspectorate's functions.
2. To participate in the development of draft laws and regulations and development planning documents and provide opinions on draft laws and regulations and development planning documents prepared by other institutions.
3. To complete and publish guidelines explaining the procedure for conducting a data protection impact assessment.
4. To complete and publish practical recommendations for individuals in the field of video surveillance.
5. To conduct preventive checks on compliance with personal data protection requirements in organizations' privacy policies.
6. To implement a public information campaign for young people in the field of data protection.
7. To take measures to promote public awareness of the processing and protection of personal data by organizing educational seminars (at least eight) and publishing explanations.
8. To fulfil the tasks specified in Sections 18 - 20 of the Data Law – to organise three examinations for data protection officers.
9. In collaboration with the Ombudsman's Office, to develop an explanation on the processing of personal data of state and municipal officials for journalistic needs.
10. To evaluate the limits of the Inspectorate's competence in matters that also affect the competence of the police, and to evaluate whether the Inspectorate should be granted the right to block websites.
11. Execution of measures included in the long-term audit plan for SIS and VIS.