Datu valsts inspekcija

ACTIVITY REPORT

2022

TABLE OF CONTENTS

FOREWORD

The Data State Inspectorate (hereinafter – the Inspectorate) has prepared a public report reflecting its performance in 2022.

This year, the Inspectorate increased its focus on one of the key priorities of its Strategy 2021–2025 (hereinafter – the Strategy), i.e., to ensure that the information available on personal data processing is comprehensible to everyone and reflects issues of public interest.

To achieve this goal, the Inspectorate has actively informed the public of the processing and protection of personal data and the rights and obligations of controllers when processing personal data through various channels in 2022. Public information activities included publications in newspapers and news portals, interviews, and participation in various radio and TV programmes. In cooperation with the media, the Inspectorate consulted and advised the public on many aspects of personal data protection, topical issues, and its decisions. The Inspectorate also sought to build a high-quality debate with data protection experts.

On 16 September 2022, the international conference "Personal Data – Future Perspective!" was held, featuring leading experts from Latvia and abroad. The conference covered issues such as the digital euro and privacy, facial recognition technologies, health data and digitalisation, cookies and available alternatives, as well as new European legislative initiatives on digital services, the digital market and data governance.

In 2022, the Inspectorate launched cooperation with the State Employment Agency within the framework of the European Social Fund (ESF) project "Support for the Education of the Unemployed" under the measure "Measures to Increase Competitiveness", organising 10 online lectures for the State Employment Agency's registered clients on data security and protection in the digital environment.

The Inspectorate also appreciates that controllers and industry experts actively consult with it to ensure appropriate solutions for the protection of personal data and compliance with the regulatory framework in atypical cases.

To ensure compliance with the laws and regulations in the field of personal data protection while encouraging controllers' full understanding of the violations they have committed, the Inspectorate has focused in 2022 on the possibility of concluding administrative agreements in cases where the controller admits the violation.

The Inspectorate was also actively involved in drafting laws and regulations, providing the drafters thereof with its views on that legislation on its own rather than through the Ministry of Justice, as was the previous practice.

1. BASIC INFORMATION

The Activity Report has been prepared on the basis of Article 59 of the General Data Protection Regulation[1] (hereinafter – the Data Regulation)[2] and in accordance with Section 13 of the Personal Data Processing Law, which stipulates that the Inspectorate shall, on an annual basis by 1 March, submit a report on the operation to the Saeima, the Cabinet, the Supreme Court, the European Commission, and European Data Protection Board, as well as make it available on its website.

1.1. LEGAL STATUS OF THE INSPECTORATE

The Data State Inspectorate was established on the basis of the Personal Data Processing Law[3] and started its activities on 1 January 2001.

Pursuant to Section 3 of the Personal Data Processing Law (hereinafter – the Data Law), the Data State 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.

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

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

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

1.2. OBJECTIVES AND FUNCTIONS OF THE INSPECTORATE

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

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

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

1. **An informed, motivated society and breaches remedied promptly.**

This line of action promotes the public visibility of the Inspectorate, and it works to increase both the public's awareness of its rights in the area of personal data processing, as well

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

[2] Article 59 of the Data Regulation: Activity reports. Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

[3] The Personal Data Protection Law has now expired.

as the personal data processors' awareness of their obligations. It also aims to promote a common approach to personal data protection measures through guidelines, recommendations, clarifications and binding public administration rules.

This line of action is particularly important because only an informed public can exercise its rights effectively, and only informed controllers can effectively fulfil their obligations. The mutual voluntary exercise of rights and obligations results in the timely identification and rectification of data processing violations and it is the most effective way of ensuring the right to personal data protection without the direct involvement of a supervisory authority.

2. Effective monitoring of personal data.

This line of action ensures that the Inspectorate's decisions and penalties are clear, transparent and fair. As a result, data controllers are motivated to comply with the requirements for processing personal data set out in the laws and regulations.

3. An efficient and development-oriented authority.

Under this line of action, the authority is committed to a values-based organisational culture that puts people at its heart and works for the public good. The Inspectorate's values – professionalism, development, cooperation, fairness and openness – contribute to achieving the Inspectorate's mission and vision, shape the organisation's environment and culture, determine the perception and mind-set of employees, which is reflected in the actions and attitudes of each employee, contribute to the return on investment, enhancing the professionalism of employees and establishing effective communication channels with society.

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

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

2. KEY TASKS FOR THE REPORTING YEAR

During the reporting year, the Inspectorate set and completed a number of tasks essential for its development and the right to protection of personal data processing.

1. The Inspectorate’s capacity was reinforced by creating a competitive and favourable working environment and engaging professional and motivated employees in the performance of its functions.
2. The Inspectorate participated in the drafting of laws, regulations and development planning documents and provided opinions on draft laws, regulations and development planning documents prepared by other institutions.
3. It carried out preventive controls on the use of cloud computing in the public sector and on compliance with personal data protection requirements in telemarketing and credit bureaus.
4. Efforts were made to validate and publish the criteria set out in Article 41(3) of the Data Regulation for the accreditation of supervisory bodies for codes of conduct.
5. In accordance with the delegation contained in Section 22, Paragraphs two and three of the Data Law, Regulation No 488, Regulations on the Licensing of the Code of Conduct Supervisory Body, was drafted and adopted by the Cabinet on 9 August 2022.
6. An international conference on current issues in data protection was organised.
7. The public awareness campaign “Your Data – Your Security” (https://www.dvi.gov.lv/lv/tavi-dati-tava-drosiba) was implemented.
8. Awareness-raising on the processing and protection of personal data was carried out through educational seminars and the publication of explanations.
9. Three data protection specialist examinations were held.

3. THE INSPECTORATE'S INVOLVEMENT IN THE IMPLEMENTATION OF THE DATA REGULATION'S REQUIREMENTS AT THE NATIONAL LEVEL

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

The reporting year was significant in that the Inspectorate started issuing opinions on draft legislation directly, rather than through the Ministry of Justice, as was the previous practice.

Although all ministries were informed of the new procedure, the Inspectorate found that it was not involved in the harmonisation of laws and regulations in all cases where a regulation affected issues within the Inspectorate's competence, so, in the reporting year, the Inspectorate requested the *Saeima* and the *Saeima* Legal Bureau to invite the authority to provide its opinion in cases where draft legislation before the *Saeima* concerned the processing of personal data and the development of new information systems, in particular where ministries had failed to comply with the procedure for the approval of draft legislation laid down in the laws and regulations.

A total of 64 draft laws and regulations were received for harmonisation on the TAP portal in 2022, with 151 opinions issued on these acts (56 initial opinions and 95 repeated opinions).

In addition, in accordance with Paragraph 7 of the Cabinet Regulation No 597, Procedures for Supervising Development Projects for State Information Systems, of 31 August 2021, when developing a new information system, a favourable opinion on the description of the State Information System development activity must be obtained from the Inspectorate. The Inspectorate issued 14 opinions on the descriptions of State Information System development activity in the reporting year.

In the reporting year, the Inspectorate provided support to the Ministry of Finance in the development and harmonisation of the Cabinet Regulation No 396, Regulations Regarding the Requirements for Updating Information in the Shared Know-Your-Customer Utility and the Licensing and Supervision of the Shared Know-Your-Customer Utility Service Provider, of 5 July 2022. It was developed to ensure the regulation on the licensing and supervision of closed and open know-your-customer utility service providers contained in the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing. Licensing and supervision of their activities under this framework are carried out by the Inspectorate.

The Inspectorate continued to take part in the development of the regulatory framework on the processing of data to be retained in the Electronic Communications Law. The new Electronic Communications Law was adopted by the *Saeima* on 14 July 2022 and entered into force on 29 July 2022. At the same time, given the Inspectorate's objections to the inconsistency of the developed regulation on data to be retained with the findings established in the case law of the European Union, it was agreed that Paragraph 18 of the Transitional Provisions of the Law requires the Cabinet to submit to the *Saeima* by 31 December 2022 a draft law to ensure that the regulation on retained data contained in Sections 99, 100 and 101 of this Law complies with the legal framework of the EU and the Constitution of the Republic of Latvia. To ensure compliance of the regulation on the data to be retained, a working group was set up to discuss the necessary changes to the framework to bring it in line with the legislation and the case law of the European Union.

During the reporting year, efforts to improve the legal framework for identity theft within the Ministry of Justice's Permanent Working Group on Criminal Law continued. During its meetings, the Working Group discussed, inter alia, whether the existing regulation in

Section 145 of the Criminal Law on illegal activities involving the personal data of natural persons also covers identity theft. The Inspectorate took the view that identity theft clearly includes the processing of personal data, but that it is not limited to data processing as such, but also to impersonating another person and performing acts on their behalf, thereby violating the integrity of that person's identity. The Inspectorate, therefore, proposed that a separate provision be introduced in the Criminal Law providing for liability for identity theft.

4. MONITORING AND INSPECTION OF THE PROCESSING OF PERSONAL DATA

4.1. PREVENTIVE INSPECTION IN THE FIELD OF TELEMARKETING

In 2022, the Inspectorate, on its own initiative, raised the issue of compliance with personal data protection requirements in the field of telemarketing, with a particular focus on identifying the sources of data acquisition, as well as their storage, use and transfer. The Inspectorate carried out a preventive inspection to verify the lawfulness of personal data processing in the private sector. This inspection aimed to ascertain whether the Data Regulation and the Law on Information Society Services are complied with, paying particular attention to whether the conditions for processing personal data in the context of telemarketing are complied with in relation to the data sources as well as storage, use and transfer of the data obtained.

Twelve companies were selected for the inspection according to the following criteria:

1. Active company registered in the Republic of Latvia.

2. The companies' business activity is Activities of call centres (according to the statistical classification of economic activities in the European Union NACE Rev. 2) (NACE – 82.20 – this class includes the activities of: – inbound call centres, answering calls from clients by using human operators, automatic call distribution, computer telephone integration, interactive voice response systems or similar methods to receive orders, provide product information, deal with customer requests for assistance or address customer complaints; – outbound call centres using similar methods to sell or market goods or services to potential customers, undertake market research or public opinion polling and similar activities for clients) or Advertising agencies (NACE – 73.11 – this class includes the provision of a full range of advertising services s (i.e., through in-house capabilities or subcontracting), including advice, creative services, production of advertising material, and buying).

3. The companies' activities are related to telemarketing, including the operation of outbound call centres.

4. The target audience for telemarketing is considered to be natural persons.

Initially, all 12 companies were asked to provide the Inspectorate in writing with information in relation to the provision of telemarketing services, focusing on the sources of information used to make targeted calls and databases that could contain data of natural persons.

The Inspectorate received replies from 10 companies. One company replied that it does not provide telemarketing services. In one case, the reply was that the company in question was the subject of a criminal case, so its business activities were suspended and it could not respond to the Inspectorate's request in those circumstances. Two other companies failed to reply to the Inspectorate's letter and to the questions raised during the preventive inspection, as they could not be reached at their registered office or the email address provided in the public domain. Information on the unavailability of the companies was sent to the Register of Companies of the Republic of Latvia for assessment and, if necessary, for the adoption of the decision provided for in Section 314.[1], Paragraph one, Clause 2 of the Commercial Law.

Based on the information provided in the companies' replies, the Inspectorate decided to carry out in-depth on-site inspections at the premises of eight companies. Seven on-site inspections were carried out between 9 August and 7 September 2022 with procedural action reports drawn up in each case. The Inspectorate adopted a decision to initiate administrative

offence proceedings in respect of one company for failure to provide the Inspectorate with information and access to premises. This resulted in a fine.

The Inspectorate found **the least room for improvement** in the sources of information and their use to make targeted calls to natural persons. At the same time, it should be noted that the inspection found that most of the personal data is provided by customers of telemarketing services, which were not inspected during the action. It is the companies' customers who mostly obtain the data subject's consent to the processing of their data.

The Inspectorate identified **the most room for improvement** in relation to compliance with security requirements for the processing of personal data.

In 2023, the Inspectorate plans to continue the inspection of controllers, given that all the companies examined were acting as processors in the telemarketing context.

4.2. SUPERVISION OF DATA PROCESSING

During the reporting year, the Inspectorate received 708 complaints from data subjects about possible personal data breaches, 88 notifications from data controllers about personal data breaches and 69 applications from other third parties (public authorities, organisations, associations) about possible personal data breaches. Based on these complaints, notifications of personal data protection violations, and the Inspectorate's own initiative, the Inspectorate carried out a total of 865 personal data processing inspections (including initiative inspections) in the framework of administrative proceedings and administrative offence proceedings.

The decrease in the number of completed inspection cases compared to the previous reporting period is due to the fact that the Inspectorate is actively involved in public education, which results in a higher number of complaints with evidence of violations filed to the Inspectorate. At the same time, the Inspectorate observed that although the number of inspections has decreased compared to the previous reporting period, the complaints received contain information about systematic violations by controllers affecting a wider range of data subjects.

Areas inspected:

1) Processing of personal data on online social networks and other websites;
2) Video surveillance in public places, private properties, businesses and institutions;
3) Processing of personal data in the information systems of public authorities;
4) Respecting the rights of data subjects;
5) Processing of children's personal data;
6) Processing of personal data in the context of out-of-court debt recovery and credit history assessment;
7) Processing of special categories of personal data (including health data);
8) Processing of personal data by the mass media;
9) Processing of personal data in e-commerce, commercial communications and telecommunications;
10) Processing of personal data by law enforcement authorities and other public law bodies.

4.2.1. NUMBER OF COMPLAINTS RECEIVED

The highest number of complaints, 191 out of 708 received during the reporting period, concerned the processing of personal data on online social networks and other websites. In most cases, processing of personal data was identified and data subjects were informed of their rights, including the right to make a request to the controller about the processing of their personal data and the right to ask the platform to erase their personal data. In particular, it was observed that individuals who have doubts about unlawful data processing do not use the mechanism provided for in the Data Regulation to defend their rights by contacting the data controller, nor

do they use the possibilities provided on social networking platforms to request the deletion of information, but rather contact the Inspectorate immediately.

The second most frequent area of complaint was video surveillance. Moreover, compared to previous reporting periods, issues related to video surveillance are becoming more apparent as video surveillance equipment is rapidly developing and becoming more affordable. When examining this type of complaint, as in the previous reporting periods, it was found that most often no information signs on video surveillance were displayed or the information sign did not contain all the necessary information required by Section 36, Paragraph three of the Data Law (name of the controller, contact details, purpose of data processing, as well as an indication of the possibility to obtain other information specified in Article 13 of the Data Regulation). In addition, it was found that in some cases controllers did not accurately identify the legal basis for processing personal data, for example by considering that processing was based on the data subject's consent. In addition, there was an increasing trend during the reporting period in the number of complaints about audio recording during video recording. Given that audio recording may significantly affect a person's privacy, in all inspections carried out by the Inspectorate where video surveillance was accompanied by audio recording, controllers were obliged to stop audio recording.

Compared to 2021, the number of complaints about the processing of personal data in the information systems of public authorities has decreased, with a total of 82 complaints received and handled in this area.

In 2022, the Inspectorate applied corrective measures (warning, order, reprimand, restriction of processing) in 234 cases when dealing with complaints from data subjects, calling on controllers to comply with their obligations under the Data Regulation. This included obligations on controllers to comply with the data subject's request, to implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is carried out in accordance with the requirements of the Data Regulation, to align the personal data processing activities with the provisions on rectification or erasure of personal data or restriction of processing laid down in the Data Regulation.

In general, the Inspectorate continues to receive many complaints from individuals about the alleged unlawful processing of personal data arising from interpersonal conflict. Examples include creating fake profiles of the data subject on social networks, publishing private photographs on various websites, and video surveillance of neighbours.

Additionally, complaints received by the Inspectorate regarding possible personal data processing violations in 2022 evidence that a large part of these violations is related to technical and organisational measures inadequately implemented by the controller to ensure the security of personal data. For example, the controller does not review and update security measures for working with information systems.

4.2.2. NOTIFICATION OF PERSONAL DATA BREACHES

In accordance with Article 33(1) of the Data Regulation, in the event of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (the Inspectorate), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In 2022, the Inspectorate received 88 notifications of personal data breaches, of which 86 contained information on breach of confidentiality, 3 – on breach of integrity, and 7 – on breach of availability.

During the reporting period, the Inspectorate received several personal data breach notifications containing information on the unlawful acquisition and publication of personal data at trading venues. In particular, the security guards of those trading venues filmed the video surveillance footage on their personal smart devices and posted it on various social networks.

4.2.3. DECISIONS TAKEN IN ADMINISTRATIVE OFFENCE CASES

In the reporting period, the Inspectorate adopted 16 decisions in administrative offence cases, imposing a fine in 12 cases, issuing a warning in three cases and terminating the proceedings in one case.

In the year under review, the range of fines imposed in administrative offence cases varied between EUR 200 and EUR 1.2 million. In 2022, the Inspectorate imposed fines totalling EUR 1 223 059.13.

These fines were imposed for offences provided for in Article 83(5) of the Data Regulation.

In three cases, for violations of the basic principles for processing (Article 83(5)(a)).

In one case, for breach of the data subject's rights pursuant to Articles 12 to 22 (Article 83(5)(a) and (b) of the Data Regulation).

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

In four cases for violation of Article 83(5)(e).

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

In one administrative offence case, the proceedings were terminated on the grounds that the circumstances provided for in Section 119, Paragraph one, Clause 1 of the Law on Administrative Liability did not allow the proceedings: there was no event or it did not contain the constituent elements of an administrative offence.

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

4.3.1. CONTESTATION

The Director of the Inspectorate took a total of 15 decisions in 2022. Of these, four decisions taken by an official were appealed in administrative offence proceedings, while 11 decisions taken by an official were challenged in administrative proceedings.

As regards the appealed administrative offence cases, in two cases the Director took a decision to amend (reduce) the amount of the fine, while the remaining two decisions upheld the appealed decision.

At the same time, with regard to the administrative procedure cases contested before the Director, it should be noted that seven decisions declared the actual action lawful, one decision upheld the administrative act, two decisions declared the actual action unlawful in part – in one case, the annulled part provided the applicant with another actual action, and the relevant Inspectorate Unit was instructed to provide an explanation, and in the other case, the decision declared the actual action unlawful and referred the application to the relevant Inspection Unit for repeated hearing.

4.3.2. APPEAL

A total of 14 final court rulings were issued in the reporting year. Of these, three were in administrative offence cases and 11 in administrative proceedings.

One of these rulings is unfavourable to the Inspectorate in an administrative offence case based on procedural irregularities committed by the Inspectorate. 10 court rulings are in the

Inspectorate's favour, while three administrative proceedings were closed due to the parties concluding administrative agreements and withdrawing their applications to the court.

Of the 14 cases, only four have been appealed in cassation and only one of these four has been reviewed in cassation on the merits. In the remaining cases, cassation proceedings were refused.

One case that may be of interest to the wider public concerns an applicant who complained about alleged unlawful data processing by a pre-school education institution. The applicant filed an application to the Inspectorate stating that a folder containing the names of all children and parents and the parent's signatures was publicly available on the premises of the educational institution. The Inspectorate explained to the applicant that in the present case, no automated processing of the applicant's personal data was carried out with regard to the accessibility of the folder to other visitors of the pre-school educational institution, nor was it established that the processed personal data form part of a filing system or are intended to form part of the filing system. Drawing up a list and the possibility for parents of children to see the names and signatures of other children and parents at a certain moment, e.g. when signing the list for compliance with the internal rules of the educational institution, does not fall within the material scope of the Data Regulation and, although such information contains personal data, would not constitute processing of personal data which would put the individual's privacy at additional risk or otherwise infringe the rights of those individuals. As the material scope of the Data Regulation was not established in this case, the Inspectorate was not competent to assess the possible violation of personal data processing.

The applicant appealed against the Inspectorate's decision to the court, where the decision of the Administrative District Court held that the Inspectorate's decision was lawful and justified and that the applicant's complaint should be rejected. The Court held, inter alia, that the availability of the name and signature of a person as an identifier was not sufficient to establish the processing of a structured set of personal data, thus not finding that the personal data formed part of a file system. The Court also recognised that an educational institution is a public environment where a person is not isolated from the influence of others; data protection is not absolute, as to a certain extent data protection has to be balanced with other fundamental rights of the person, such as the right to education.

5. CASE STUDIES

5.1. FAILURE TO COOPERATE WITH THE SUPERVISORY AUTHORITY

The number of penalties imposed for failure to cooperate with the supervisory authority has increased during the reporting period: In 2021, the Inspectorate imposed two administrative fines for non-cooperation, while in 2022, 11 fines were imposed for this type of violation, of which five were for non-compliance with the Inspectorate's requests and six for failure to provide the Inspectorate with information.

These cases involved fines for both legal and natural persons. As regards the specific cases in 2022, the sanctioned persons failed to provide the Inspectorate with information on the processing of personal data on social networks and video surveillance, thus preventing the Inspectorate from verifying that such processing complies with the requirements of the Data Regulation.

5.2. PROCESSING OF PERSONAL DATA ON DATING SITES

During the reporting period, the Inspectorate received numerous complaints from citizens regarding the unlawful actions of others who uploaded and distributed personal data of data subjects on various dating and intimate content websites without obtaining informed consent.

Third parties with malicious motives used data subjects' personal data, such as name, surname, telephone number, facial image, and e-mail address, on various dating and intimate content websites without obtaining consent, which allowed visitors to contact the data subject using the contact details provided in the advertisement. As a result of these activities, data subjects received various unpleasant and often vulgar messages, even though they had not registered or taken any action on the websites in question.

Based on the information provided in the complaints, the Inspectorate identified an element of regularity, as a result of which the Inspectorate approached the website administrators (hosts) with a request to remedy deficiencies on their websites, as well as to introduce additional measures at the time of profile registration and advertisement placement, such as providing a telephone number and e-mail address attached to the advertisement, mechanisms to verify the text included in the text section, both to allow visitors to take the actions they want by confirming the contact details added to their profile, and to reduce the tools available to third parties to prevent them from taking revenge on another person, such as an ex-spouse, colleague or neighbour, for personal motives.

In addition, in the above-mentioned cases, the Inspectorate addressed the hosts of the websites and asked them to stop the unlawful processing of personal data on the websites in question using cookies and other tracking technologies.

5.3. PROCESSING OF PERSONAL DATA ON WEBSITES USING COOKIES

In 2022, the Inspectorate inspected a number of websites for their use of cookies, both on the basis of complaints received and on its own initiative, initiating administrative offence proceedings for unlawful processing of personal data through cookies on websites managed by hosts in two cases. In particular, cookies from these websites were placed on users' end equipment without them being informed and providing their consent in accordance with the Data Regulation and the Law on Information Society Services (LISS), and without them giving them the opportunity to change their consent or refuse further use of cookies at any time.

In both administrative proceedings, the Inspectorate found that, as a result of such processing of personal data, the companies had violated a number of fundamental principles set out in Article 5 of the Data Regulation, and that the processing of personal data was carried out without the legal basis set out in Article 6(1) and in breach of the conditions of lawful (including

informed, unambiguous and free) consent set out in Article 7, as well as the conditions laid down in Section 7.[1] of the special law – LISS – which must be complied with when personal data are processed using cookies or other technologies which allow the user to be identified and their activities to be tracked, not only on the website in question but also on other unrelated websites.

Given that both companies immediately remedied the cookie violations detected by the Inspectorate after the administrative offence proceedings were initiated, including by closely following the Inspectorate's recommendations in its Guidelines on the use of cookies on websites, and showed a high level of cooperation with the supervisory authority, the Inspectorate issued warnings to the companies in both cases.

5.4. PROCESSING OF PERSONAL DATA BY AN INTERNATIONAL CHAIN OF STORES ON THE BASIS OF CONSENT PROVIDED BY CUSTOMERS

During the reporting period, the Inspectorate cooperated in a number of cases with data supervisory authorities in other countries, both in the exchange of information and in the adoption of final decisions in cases under its competence and pending before it. In the framework of this international cooperation procedure *(One-Stop-Shop*), in 2022 the Inspectorate, as the lead supervisory authority, completed an inspection of complaints received about the practice of a company operating in all three Baltic States of issuing a customer card without obtaining the customer's consent in accordance with the legal framework.

To receive additional services offered by the company, such as home delivery, the customer was required to have a customer card as a prerequisite. But to obtain the customer card, the customer had to "consent" to the processing of his personal data for a number of unrelated purposes, such as the issuance of an accounting source document, the identification of the customer, and other purposes. In addition, the personal data to be included in the application form had to be provided to the maximum extent necessary to achieve all these purposes: name, surname, personal identification number, date of birth (for non-residents), business registration number, address and telephone number.

Considering that a customer who has not given his consent to the issuance of a customer card could not receive additional services, the Inspectorate concluded that the company does not comply with the definition of consent set out in Article 4(11) of the Data Regulation. In particular, consent cannot be considered freely given if the withholding thereof results in the unavailability of the service. The Inspectorate also found that the company processes personal data for different, mutually separable and unrelated purposes by asking customers for their consent in a single questionnaire, which requires the person to provide their personal data for all purposes, thus violating the data minimisation principle set out in the Data Regulation. In light of the violations established during the inspection, the Inspectorate found the company guilty of an administrative offence under Article 83(a) of the Data Regulation and imposed a fine.

5.5. PROCESSING OF PERSONAL DATA DURING THE CONCLUSION OF A SERVICE CONTRACT

In the reporting year, the Inspectorate examined an administrative offence proceedings case concerning the conduct of an electronic communications merchant offering customers to conclude a service contract remotely without verifying the customer's identity.

In the course of the case's examination, the Inspectorate found that, when developing the services available to customers, the merchant developed and introduced the possibility for customers to apply for and conclude a contract for the provision of services remotely. To apply for and conclude a contract remotely, a person had to fill in their name and contact details and later confirm the contract using the authentication tools developed by online banks on the merchant's website. The Inspectorate found that the service was available to clients immediately

after completing the application, even in cases where the client did not confirm the contract, and that the person was regularly invoiced for services on the basis of an unconfirmed contract. At the same time, the Inspectorate found that in at least one case, the personal data contained in an unconfirmed contract had been transferred to a third party to initiate debt recovery proceedings. Thus, the Inspectorate found that the processing (acquisition, storage and transfer) of personal data of such customers took place without the legal basis set out in Article 6(1) of the Data Regulation.

The Inspectorate's examination of the case also showed that when receiving an application from a new customer, the merchant compared the personal data included in the application with the historical and archival data available to the merchant, for example, if the person had previously been a customer of the merchant, and included the historical personal data available thereto in the new service provision contract, rather than the personal data provided by the person in the application. The Inspectorate thus concluded that such conduct of the merchant may facilitate the transfer of customer data to third parties, in particular, if the customer's data were used illegally by third parties in the service application. In addition, such processing may also result in third parties being in possession of data that they did not have before. Consequently, the Inspectorate found that the trader had violated Article 5(1)(a) and (f) of the Data Regulation.

In this case, the Inspectorate found that at the time of the hearing, the merchant had already made the relevant improvements to ensure that a person's identity is confirmed if they wish to apply for a contract remotely; however, given the gravity of the violations found and other circumstances assessed in the case, the Inspectorate imposed a fine on the merchant.

5.6. PROCESSING OF PERSONAL DATA BY A SWORN ATTORNEY

On the basis of a complaint from a person regarding the processing of their personal data in legal proceedings, the Inspectorate examined a case in which it found that a sworn attorney (attorney A), representing his client in legal proceedings, obtained a certificate from the Office for Citizenship and Migration Affairs (the Office) containing the following data of four persons: name, surname, personal identification number and the relationship between them. The information contained in the certificate was essential to prove the subject-matter of the action and was submitted to the court (court proceedings A). Another attorney (attorney B), who was also a representative in court proceedings A, obtained the certificate requested by attorney A and submitted it in another court proceeding (court proceedings B). It was found that the plaintiff in court proceedings B was a company owned by and represented by attorney B, and the details of only two of the persons included in the certificate issued by the Office were relevant in court proceedings B.

The Inspectorate concluded that an attorney has the right to obtain evidence, including documents from the Office containing personal data and attesting to a particular fact. In the present case, by contrast, attorney B unlawfully obtained the certificate requested by attorney A and submitted it in court proceedings B. In accordance with the parties to the proceedings' right of access to the file, the personal data in the certificate were accessible to the parties to court proceedings B, including the two other persons who were not parties to the proceedings. In the case, the Inspectorate imposed a corrective measure – reprimanded the law firm where attorney B practised during court proceedings A for failing to ensure that litigation files in its records were not illegally transferred to third parties and attorney B's firm, as well as for illegally obtaining, transferring and storing the data of two persons not related to court proceedings B included in the certificate. The Inspectorate noted that attorney B could have obtained the necessary evidence for court proceedings B independently by contacting the Office and requesting evidence of certain content. In such a case, the Office would assess the justification of the request and issue a certificate containing only the data of the persons necessary for court proceedings B.

5.7. PROCESSING OF PERSONAL DATA BY THE EMPLOYER

In 2022, the Inspectorate completed an inspection of a case where the employer had requested written proof of vaccination against Covid-19 from employees as part of the national epidemiological measures, indicating the name of the vaccine and the date of vaccination. In addition, the Inspectorate found from the case file that the employer provided detailed information on the absences of employees in the employee work schedule, available to all employees, indicating the employee's name, surname, and the reason for absence, e.g. sick leave, additional leave for a child.

As regards the processing of Covid-19 vaccination data, the employer justified this on the basis of the government's plans to set an expiry date for interoperability certificates. Therefore, given the nature of the employer's activities and the number of employees, it decided to obtain the data in time to ensure the continuity of its operations. The data were only accessible to those employees who needed it to do their job, and would be destroyed if the requirements for interoperability certificates were removed.

The Inspectorate found that in the present case, the processing of special categories of data was based on assumptions about possible changes in the legislation although there was no political agreement yet on the implementation of these changes. Taking into account the detailed list of cases in which processing of special categories of personal data is permissible in Article 9(2) of the Data Regulation, the Inspectorate concluded that it cannot be based on the statements or plans of individual politicians. At the same time, the Inspectorate drew the attention of the controller to the fact that in the given case, taking into account the epidemiological measures established in the country, the employer had the right to be informed whether employees met the requirements to perform the duties of their posts, however, the employer could not require such a statement to include the amount of information exceeding that required by the laws and regulations. As regards the detailed transcription of employees' absences, the Inspectorate drew the controller's attention to the fact that information on the reasons for employees' absences should be available only to those employees who need it for the performance of their duties, but if this information is available to a wider range of persons, the employer is over-processing (indirectly disclosing) the private data of its employees.

In the case in question, the Inspectorate imposed a corrective measure – a reprimand – on the controller and ordered it to delete the Covid-19 vaccination data in its possession and to update the work schedules so that information on the reasons for absence was not accessible to all employees.

5.8. PROCESSING OF CHILDREN'S PERSONAL DATA IN AN EDUCATIONAL INSTITUTION AND ON SOCIAL NETWORKS ON THE INTERNET

The Inspectorate carried out an inspection on the processing of children's personal data in an educational institution upon receiving a complaint from a person. During the inspection, the Inspectorate found that a teacher of the educational institution had published on their private social network profile (account) photographs from various school and extracurricular events showing, inter alia, children from the teacher's class.

When assessing the lawfulness of the processing of children's personal data, it was found that consent under Article 6(1)(a) of the Data Regulation had been obtained by the educational establishment, however, the teacher did not have such consent to process children's personal data.

In this case, the Inspectorate drew the attention of the local government that established that educational institution to the fact that the institution must obtain consent for the processing of personal data carried out by itself, for example on its social network page. At the same time, the educational institution is not required to obtain consent for the processing of personal data by the teacher on their private social network profile, as the teacher in such a case is considered to be a separate controller acting arbitrarily.

At the same time, the inspection revealed that the personal data processing rules drawn up by the educational institution do not provide full information on the processing of personal data it carries out, for example, not all the purposes of personal data processing were defined or the legal basis for the processing of specific personal data was not indicated.

The Inspectorate imposed a corrective measure – a reprimand – on the controller and asked it to remedy the deficiencies, while the Inspectorate asked the teacher in question to obtain the consent of the children's parents to process their children's personal data or to delete the children's photos from their personal social network profile.

5.9. DESTRUCTION OF DOCUMENTS CONTAINING PERSONAL DATA

In 2022, a person submitted to the Inspectorate a set of documents which had been dumped in a waste container outside a medical institution. The documents were found to be various documents related to medical treatment, issued to different persons over several years. Some of the documents were fully intact, but others were torn into two or more pieces. As a result of the inspection, the Inspectorate found that the issuers of the documents are three different legal entities (controllers) providing medical services in one health centre.

Given that the Inspectorate was unable to establish the circumstances under which the medical documents ended up in the waste container, including the person responsible for throwing them away, the Inspectorate concluded that the documents were probably forgotten by the patients at the health centre and kept by someone employed at there with the idea that the patients might come to collect them. As no one came for the documents, the person decided to throw them in the trash.

In view of the above, the Inspectorate did not impose a corrective measure on the controllers during the inspection but instead asked them to remind the employees that the documents containing personal data should be destroyed with sufficient care, for example, by shredding them and not by throwing them in the trash.

5.10. PROCESSING OF PERSONAL DATA IN INFORMATION SYSTEMS

On its own initiative, the Inspectorate carried out an inspection of the information system maintained on the website of a company, which had published and made available the registration and other documents containing personal data of natural persons to be submitted to the Enterprise Register of the Republic of Latvia (hereinafter – the Register) and to be included in the non-public part of the Register's registration file.

During the inspection, the Inspectorate found that when logging into the information system and randomly checking the available information about a particular company, scanned documents with personal data are available for downloading, which have been placed in the information system in violation of the provisions of Section $4.^{15}$, Paragraph one, Clause 3, Sub-clause a of the law On the Enterprise Register of the Republic of Latvia, i.e. they are to be included in the non-public part of the Register's registration file and cannot be made available for re-use.

The company explained that in December 2019, in preparation for the entry into force of the amendments to the relevant legislation, it carried out file deletion and, after retesting the deletion results, it found that some document files had not been deleted. The identified cause was due to temporary network interruptions during the deletion process when several data arrays were fed to the backup at the same time. The deletion procedure was designed to delete files sequentially by company registration number, and so these interruptions resulted in the failure of processing (deleting) a specific set of files.

In addition, the company pointed out that after the transition to the latest version of the information system, the non-publishable data of any company's registration file are no longer available, as the new system automatically filters and prevents the publication of documents included in the non-public part of the Register's registration file even in cases where the Register

would send such data in error. The company remedied the breach by deleting the accessible personal data.

Having assessed the nature, gravity and duration of the violation, the number of data subjects affected and other circumstances of the case, including the company's admission of guilt and the prompt action taken to remedy the violation, the Inspectorate imposed a warning on the controller.

5.11. CASES WHERE THE INSPECTORATE ASSESSED THE BALANCE BETWEEN THE INDIVIDUAL'S RIGHT TO DATA PROTECTION AND THE PUBLIC INTEREST, OTHER FUNDAMENTAL RIGHTS OR LEGITIMATE INTERESTS OF THE CONTROLLER

In the reporting year, the Inspectorate gave its opinion in cases where the balance between the individual's right to data protection and the public interest had to be assessed, such as in the case of the processing of police officers' data on social networks.

In one case, a police officer on their job was called to a family conflict and the conflict was streamed live on a social networking app. At the time the police officer contacted the Inspectorate, the video from the scene was no longer available on the original poster's profile. However, some parts of the video had been saved by another user and republished on their profile, splitting the original online streaming recording into several parts.

Given that the event took place at a time when various epidemiological measures were in force, the police officer was wearing a mask covering the mouth and nose and the patch attached to his uniform was not visible during the recording, the police officer was not identifiable in several videos and such data processing does not fall within the scope of the Data Regulation. At the same time, taking into account that in some of the videos the police officer was saying his name out loud, the Inspectorate concluded that the processing of the data in the videos in question did not comply with Section 32, Paragraph two of the Data Law, as in this case the online streaming video showed a video and sound recording of a family conflict, which the police were called to resolve.

In the second case, the police officer had summoned the parties to an administrative offence hearing. The persons had started an online streaming video on a social networking app when they arrived at the police office, and the video showed all third parties and police officers visiting the police station at that moment, who were not related to the case in question.

In assessing the case, the Inspectorate concluded that the purpose of the persons who arrived at the police station and started the online streaming video was to provoke the police officer to a possible unlawful act, as the persons' actions were provocative, often violating generally accepted norms of behaviour. The Inspectorate concluded that in this case, too, the processing of the police officer's data did not comply with Section 32, Paragraph two of the Data Law, including that in this case the police officer's right to data protection outweighed the public interest, as the purpose of the video in question was to discredit the officer in question.

6. INTERNATIONAL COOPERATION

6.1. ONE-STOP SHOP

In 2022, the IMI system handled a total of 554 applications received in line with the procedure of Article 56 of the Data Regulation (identification of the lead and participating authority). The Inspectorate was involved in a total of 13 cases, including five where the Inspectorate was been designated as the lead authority and eight where the Inspectorate was designated as a participating authority. One of the cases where the Inspectorate was the lead authority had an inspection completed and a decision taken in 2022.

In the framework of international cooperation, the Inspectorate, as a potentially involved or relevant supervisory authority in the case, offered assistance in assessing breaches to data protection authorities of other EU Member States, for example, to the Dutch authority in relation to an inspection of a transfer of personal data to the Russian Federation by a data controller that was still active in Latvia at the beginning of 2022.

6.2. ENSURING CONSISTENCY

To ensure consistency, the Inspectorate has harmonised with the European Data Protection Board (EDPB) the Inspectorate's criteria for accreditation of certification authorities (bodies) in 2022. The EDPB also provided its opinion on the criteria for the accreditation of supervisory authorities (bodies) for codes of conduct.

In 2022, the Inspectorate was active in the development of the EDPB working documents, acting as lead reporting authority on two working documents and as co-rapporteur on another two working documents.

Of particular note is the Inspectorate's performance in the first EDPB-coordinated inspection. The inspection focused on the use of cloud solutions by the public sector. It aimed to promote best practices in the use of cloud services in the public sector, thereby ensuring adequate protection of personal data.

An intermediate conclusion on the results of the inspection in Latvia identified the need to improve organisations' knowledge about cloud services and their role and risks in the processing of personal data, as it was found that not all organisations understand the concept of cloud services and can identify which service is cloud-based.

The Inspectorate fully agrees with the opinions published by the EDPB, where recommendations were made to improve the compliance of personal data processing activities as a whole.

6.3. COOPERATION BETWEEN BALTIC SUPERVISORY AUTHORITIES

Several coordinated supervisory activities were implemented in 2022, as agreed by the supervisory authorities of the Baltic States at the 2021 Baltic Supervisory Authorities Meeting, during which the authorities agreed to conduct sectoral monitoring to develop recommendations to improve the processing and protection of personal data in a pre-agreed sector.

The authorities agreed that traders offering short-term rentals of vehicles, including electric scooters, whose main recipient is a natural person, would be inspected.

The primary focus would be on traders whose main place of business is in one of the Baltic States and who offer their services throughout the Baltics. At the same time, each supervisory authority, in line with its independence in decision-making, would be allowed to extend the scope of the inspection to the activities of merchants active in only one Member State.

The analysis of the inspection results revealed that certain aspects of processing require more in-depth analysis. Particular attention should be paid to the appropriate use of the legal basis in cases where processing is based on the protection of the legitimate interests of the

controller, as well as to the processing of biometric information. It also identified the need to focus on analysing the security and functionality aspects of the applications used.

The supervisory authorities agreed to take note of and act on the information received so far in the framework of the sectoral monitoring and to continue the coordinated inspection activities, focusing on an in-depth assessment of the above aspects that have proved problematic for all supervisory authorities.

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

In addition to the tasks set out in the Data Regulation, the Inspectorate is obliged to monitor the processing of natural persons' data in large-scale European Union IT systems in accordance with specific laws and regulations.

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

During the period 2022, preparations were made for the supervision of personal data protection requirements in the large-scale IT systems planned to be operational in 2023, i.e., ECRIS – European Criminal Records Information System, ETIAS – European Travel Information and Authorisation System and the Framework – which ensures interoperability of the data stored and processed in these information systems.

6.4.1. SCHENGEN INFORMATION SYSTEM

In 2022, an inspection was carried out on the compliance of the alerts entered in the system with the conditions of Article 36 of the SIS II Decision. The inspection did not reveal any non-compliance with the procedure for creating and entering alerts into the system.

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

As part of its monitoring activities, the Inspectorate organised a training seminar for State Police officers involved in international cooperation. The seminar provided an introduction to data protection and the distinction between the scope of the Data Regulation and the legislative act transposing the Police Directive.

The audit was closed in 2022 and the process of agreeing on a plan to address the non-conformities identified in the audit was initiated.

6.4.2. VISA INFORMATION SYSTEM

In 2022, an inspection was carried out on the processing of information at one of the endpoints of connecting to the system, the Riga Airport. The inspection did not reveal any non-compliance with the logical and physical security requirements of the State Border Guard for the operation of the system.

An inspection was carried out on the compliance of the standard answers to data subjects used by the Office of Citizenship and Migration Affairs with the laws and regulations governing the operation of the VIS. As part of the inspection, copies of the standard replies were obtained and analysed for compliance. Some additions were identified as necessary and were successfully implemented.

As part of its monitoring activities, the Inspectorate organised a training seminar for State Border Guard employees involved in international cooperation. The seminar provided an introduction to data protection and specific details of working with large-scale information systems and the highly regulated area of the civil service. The training emphasised the

obligation of employees to carefully follow the procedures developed and introduced by the employer.

In 2022, following the suggestions made by the European Commission during the previous evaluation mission, an on-site visit to one of the Latvian embassies dealing with visa issuance was also planned to assess the security and compliance of the processes in place. Such an inspection in 2022 was also planned for Ukraine but failed – initially due to the Covid-19 restrictions, and later in the year, in relation to the situation in Ukraine.

The audit was closed in 2022 and the process of agreeing on a plan to address the non-conformities identified in the audit was initiated.

6.4.3. EUROPEAN DACTYLOSCOPY DATABASE FOR ASYLUM SEEKERS (EURODAC)

During the 2022 monitoring activities, the Inspectorate examined what the relevant authorities have done to remedy the non-compliances identified in the previous audit report and implement the recommended improvements. The follow-up did not reveal any deviations from the agreed implementation plan.

6.4.4. INFORMATION SYSTEMS EXPECTED TO BE OPERATIONAL IN 2023

The Inspectorate carried out an analysis in 2022 on the amount of information that should be provided to data subjects both by the supervisory authority and by the authorities that will use these systems. The internal procedures that the Inspectorate should develop and implement for successful monitoring measures were analysed.

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

In late 2021, the Inspectorate submitted a project proposal for the European Commission's financial programme “Citizens, Equality, Rights and Values” (CERV) 2021-2027 [1] under the call for proposals No CERV-2021-DATA for personal data protection supervisory authorities to raise the level of awareness of target groups on data protection rules and their implementation. In March 2022, the European Commission approved the project proposal submitted by the Inspectorate. On 1 September 2022, the Inspectorate signed a contract with the European Commission on its implementation. The project aims to develop a distance learning programme on personal data protection for small and medium-sized enterprises, thus providing this target group with a free tool to acquire knowledge and practical skills in personal data protection and to use the knowledge in their companies. The training will provide both theoretical knowledge and practical exercises. It is planned that this training programme will be in Latvian, English and Russian. Information on the project is available on the Inspectorate's website. The distance learning programme is expected to be available in 2024.

7. THE DATA PROTECTION OFFICER

The data protection officer's main role is to support and advise organisations on the protection of personal data, resolve problems in this area and make recommendations on appropriate data processing. Article 37(1) of the Data Regulation sets out the criteria when the controller and the processor are obliged to appoint a data protection officer, while the Inspectorate continues to welcome the appointment of a data protection officer where it is not mandatory.

In 2022, 71 public sector bodies and 110 legal entities notified the appointment or replacement of 181 new data protection officers. In some cases, the same controller appointed more than one data protection officer. Of the appointed experts, 118 are included in the Data State Inspectorate's public list of data protection officers.

Three qualification examinations for data protection officers were held, testing the knowledge of potential candidates. 70 candidates took part in these exams, 23 of whom passed the examination successfully and were included in the Inspectorate's list of data protection officers. The contact details of the listed professionals were updated to ensure that the information is accurate. As the deadline for the qualification of the listed officers approached, a number of data protection officers were consulted on the steps to be taken to ensure that they are not removed from the list and that they successfully maintain their qualification.

The Data Regulation does not stipulate that only persons who have passed a qualification test organised by a supervisory authority may act as a data protection officer, this right is also extended to persons who have appropriate professional qualifications, in particular expertise in data protection law and practice and the capacity to perform the tasks referred to in Article 39 of the Data Regulation. The Inspectorate thus also advised and informed prospective professionals on how to qualify, how to ensure that their skills and knowledge are adequate, and explained to controllers that a potential data protection officer does not necessarily have to be included in the Inspectorate's list, but that passing the qualification exam may indicate that the person's knowledge is sufficiently strong. The Inspectorate also regularly drew the controllers' attention to the need to cooperate with the data protection officer appointed in the organisation, stressing that the sole reason for the appointment of this person is not to sort out the paperwork, but also to provide advice and support in everyday situations, such as when data subjects approach the organisation and ask for clarification of the compliance of the processing with the regulatory framework.

The list of qualified personal data protection officers maintained by the Inspectorate as of 31 December 2022 contains information on 376 data protection specialists who have obtained their qualification in accordance with the Data Law and the Cabinet Regulations issued by the delegation thereunder. The Inspectorate also received several verbal requests to re-include a person in the officer's list, as the person had missed the deadline of 5 January 2019 specified in the Transitional Provisions of the Data Law.

8. SUPERVISION OF CREDIT REPORTING AGENCIES

In accordance with the procedure established by the Law on Credit Bureaus and the Cabinet Regulation No 267 of 2 June 2015, Regulations Regarding Licensing and Supervision of Credit Bureaus, two credit reporting bureaus have been registered in Latvia: the joint stock company (AS) "Kredītinformācijas birojs" and the joint stock company (AS) "CREFO birojs". The purpose of the Law on Credit Bureaus is to contribute to the promotion of responsible crediting and responsible and honest borrowing, enabling the formation of personal credit history, and also to ensure legal protection of natural persons so that, upon evaluating creditworthiness, true and complete information is accessible and used. Credit reporting bureaus are licensed and supervised by the Inspectorate. Pursuant to Section 23, Paragraph one of the Law on Credit Bureaus as well as its own initiative, the Inspectorate carried out preventive inspections on the compliance of the personal data processing by credit reporting bureaus with the requirements of the Data Regulation and the Law on Credit Bureaus. The on-site inspections were carried out at the premises of AS Kredītinformācijas Birojs and AS CREFO Birojs. Overall, the preventive inspections of AS CREFO Birojs and AS Kredītinformācijas Birojs did not reveal any material non-compliance with the requirements of the Data Regulation and the Law on Credit Bureaus.

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

9. COMMUNICATION WITH THE PUBLIC

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

For the second year in a row, the Inspectorate is running an information and explanatory campaign #DVIskaidro[4] (the Data State Inspectorate explains or #DSIexplains) to provide everyone with accessible information on current issues in data protection. The #DVIskaidro feature provides weekly explanations to promote good data protection practices, with advice on how organisations (both public and private sector) can ensure they are processing data in line with the Data Regulation, and practical tips for citizens on how to exercise their rights.

In the reporting year, the Inspectorate cooperated with the media at the national and international levels to inform the public and raise awareness on the processing and protection of natural persons' data in 61 cases.

9.1. SEMINARS[5]

To ensure the public with information on current developments in data protection and to answer frequently asked questions, the Inspectorate participated in 33 seminars and conferences at the national and international levels, including online seminars on topical issues in data protection:

- On 28 January, to mark the 16th European Data Protection Day, a seminar for citizens on data subject rights under the Data Regulation, which give them more opportunities to protect their personal data;

[4] Explanations available at https://www.dvi.gov.lv/lv/dviskaidro

[5] Presentations and video recordings of the webinars are available at https://www.dvi.gov.lv/lv/prezentacijas-un-video

- On 24 March, a seminar in cooperation with the State Employment Agency for citizens on data security in the digital environment as part of Digital Week 2022;
- On 25 May, to mark the fourth anniversary of the Data Regulation, a seminar for data protection professionals and businesses on the use of cookies and conducting a data protection impact assessment;
- On 2 July, in cooperation with the State Chancellery, the Ministry of Culture and the Central Statistical Bureau, participation in the LAMPA conversation festival, organising the erudition game "Do you know or do you think you know?";
- On 27 July, a seminar for the general public on how the State Data Inspectorate monitors data processing, investigates complaints received, when it initiates inspection cases and in which cases it applies corrective measures to prevent unlawful data processing;
- On 12 October, in cooperation with the Latvian Chamber of Commerce and Industry, a seminar for entrepreneurs on preventive inspections, with an in-depth focus on obtaining consent, applying the Law on Information Society Services, technical aspects of using cookies on a website and appointing a personal data protection officer in a company.

In 2022, the Inspectorate launched cooperation with the State Employment Agency, which involved representatives of the Inspectorate giving 10 informative lectures to 648 clients of the State Employment Agency: the unemployed, job seekers, and persons at risk of unemployment. The lectures "Data security and protection in the digital environment" contained both theoretical and practical information on how to handle personal data in everyday life and the digital environment. The content and delivery of the lecture were well received by the audience, as evidenced by the discussions that took place in the Q&A section of the lecture. For more information see: https://www.nva.gov.lv/lv/jaunums/nva-sadarbiba-ar-dvi-riko-lekcijas-klientiem-par-datu-drosibu-un-aizsardzibu-digitalaja-vide. This cooperation will continue in the 2023 reporting year, with a further 11 lectures planned for the customers of the State Employment Agency.

9.2. INTERNATIONAL CONFERENCE "PERSONAL DATA – FUTURE PERSPECTIVE! 2022"

In the reporting year, the Inspectorate organised an international anniversary conference "Personal data – future perspective! 2022", bringing together leading experts from the public and private sectors to share their experiences on different aspects of the processing and protection of personal data. The conference was attended by 1658 participants in person and online.

32 leading experts from Latvia and abroad (Belgium, Germany, Austria, Great Britain, Finland) took part in the conference to share their experience on various aspects of personal data processing and protection. During the parallel sessions, experts shared their experiences and discussed the opportunities and risks in the area of personal data protection now and in the future, focusing on issues such as the digital euro and privacy, facial recognition technologies and the use of artificial intelligence, health data and digitisation, alternatives to cookies, new European legislative initiatives on digital services, the digital market and data governance.

Information about the conference is available at: https://www.dvi.gov.lv/lv/pdnp_2022

9.3. RAISING PUBLIC AWARENESS, RECOMMENDATIONS AND GUIDELINES

As part of its core functions, the Inspectorate was engaged in the daily education of the population, including foreigners, through telephone consultations, written consultations and the virtual assistant Zintis available on the Inspectorate's website. The assistant's main task is to provide customers with answers to simple, short questions within the institution's competence. In the reporting period, 407 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 who do not understand the basic function of the virtual assistant ask long questions or describe a problematic situation, resulting in an unanswered question.

In 2022, 1995 telephone consultations and 497 written consultations on data protection and processing issues were provided to both natural and legal persons, as well as to public authorities. 490 written requests for advice were received from citizens in 2022. The topics discussed most frequently during these consultations were processing in the context of employment relationships, the conditions for video surveillance of natural and legal persons, video surveillance without informing the data subject, surveillance of other private property without the consent of the owner, data processing on the web and social networks, including the processing of cookies, the implementation of data subjects' rights in practice, and data processing by the public sector. In cases of problems, data subjects were explained their rights under the Data Regulation to the protection of their personal data, including recourse to the Inspectorate.

Providing advice and educating citizens, including legal persons, (within the framework of consultations and inspections) on personal data processing issues and providing explanations contributes to the public visibility of the Inspectorate and its credibility as a public administration authority, and prevents potential violations if a controller approaches the Inspectorate with confusion about the sector's regulatory framework and basic principles of data protection or if a citizen is informed about their rights in relation to data protection. At the same time, the “advice first” principle, first implemented in 2017, is reinforced and maintained.

“Your Data – Your Security” awareness campaign

In 2022, to raise awareness of data protection and privacy and to promote good practices in data protection, the Inspectorate launched a public awareness campaign “Your Data - Your Security!” on the occasion of International Data Protection Day on 28 January, encouraging people to be responsible with their data by monitoring and controlling the transfer of their data to third parties and exercising their rights under the Data Regulation.

Information on the #TAVIDATITAVADROŠĪBA campaign and campaign leaflets is available at: https://www.dvi.gov.lv/lv/tavi-dati-tava-drosiba.

Recommendations on “Processing of personal data during the pre-election period”

In the reporting year, in preparation for the elections of the 14th Parliament of the Republic of Latvia (*Saeima*), the Inspectorate prepared and sent to political parties and their associations recommendations “Processing of personal data during the pre-election period” on measures to be taken when processing data of natural persons in the context of elections. Information is available at: https://www.dvi.gov.lv/lv/jaunums/rekomendacijas-politiskam-partijam-un-apvienibam.

Series of articles for data protection officers

In the reporting year, the Inspectorate developed a series of articles under the #DVIskaidro (#DSIexplains) feature with practical advice for future and current data protection officers on the role and status of the data protection officer, the need to designate a data protection officer in organisations and the prevention of potential conflicts of interest:

- DVIskaidro “Kas ir datu aizsardzības speciālists?” (#DSIexplains “What is a Data Protection Officer?”)
- DVIskaidro “Datu aizsardzības speciālista funkcijas un uzdevumi” (#DSIexplains “Functions and tasks of the Data Protection Officer”)
- #DVIskaidro “Datu aizsardzības speciālista kvalifikācija un interešu konflikta novēršana” (#DSIexplains “Qualifications of a data protection officer and conflict of interest prevention”)

Handbook on the processing of natural persons' data in the field of AML/CFTP and sanctions compliance

In the reporting year, the Financial and Capital Market Commission, in cooperation with the Inspectorate and Finance Latvia, developed a manual on the processing of natural persons' data in the area of anti-money laundering, combating the financing of terrorism and proliferation and sanctions compliance. The handbook explains how market participants can address the challenges of complying with both anti-money laundering and combating the financing of terrorism and proliferation and personal data protection requirements.

Detailed information available at: https://www.dvi.gov.lv/lv/jaunums/fktk-sadarbiba-ar-dvi-un-fna-izstradajusi-ieteikumus-finansu-iestadem-fizisko-personu-datu-apstradei.

Decisions, explanations and opinions of the Data State Inspectorate

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

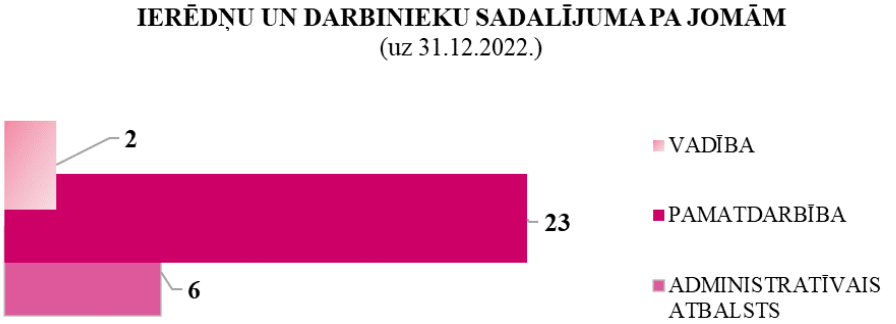
Decision database available here: https://www.dvi.gov.lv/lv/lemumi.

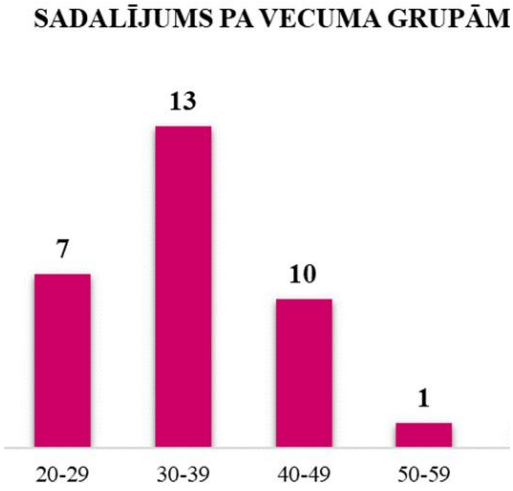
Explanations and opinions are available here: https://www.dvi.gov.lv/lv/skaidrojumi-un-viedokli.

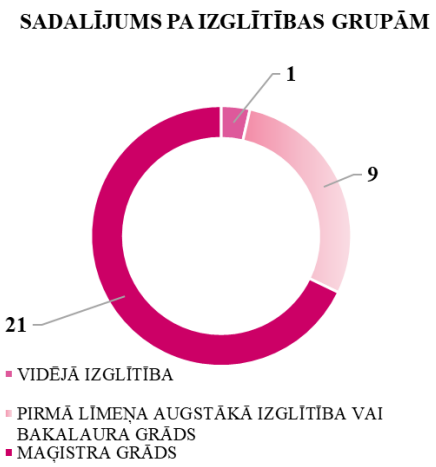
10. STAFF

During the reporting period, 35 posts and one temporary post were approved for the implementation of the European Union DLPDP project until 30 September 2024. On 1 October 2021, two posts were reallocated from the State Land Service to the Data State Inspectorate on the basis of the Public Administration Reform Plan, with funding as of 1 January 2022. These posts were allocated to the supervision of the ECRIS and ETIAS systems.

On average, 31 officials and employees, 24 women and 7 men, were employed during the reporting year.







The State civil service relationship was terminated for 4 officials. 6 State civil service officials were appointed, and an employment relationship was entered into with 1 employee.

11. FINANCIAL RESOURCES AND PERFORMANCE OF THE AUTHORITY

The authority is financed from revenue sources:
1. A grant from the general revenue
2. Paid services and other own revenue
3. Foreign financial assistance

Budget implementation is ensured by the following programmes:

- Sub-programme 09.02.00 “Data protection of natural persons”;
- Sub-programme 70.15.00 “Implementation of projects and actions under other EU policy instruments (2021-2027)”.

The use of funds and the achieved indicators in 2022 and their comparison with 2021 in the sub-programme 09.02.00 “Data protection of natural persons” are presented in Table 1.

TABLE 1

SUB-PROGRAMME 09.02.00 “DATA PROTECTION OF NATURAL PERSONS”

No.	Financial indicators	Previous year (actual implementation), *euro*	Reporting year, *euro*	
			approved by law	actual implementation
1.	Financial resources to cover expenditure (total)	1,141,077	1,450,603	1,402,837
1.1.	grants	1,136,650	1,433,276	1,394,908
1.2.	paid services and other own revenue	4,426	17,327	7,929
2.	Expenditure (total)	1,139,970	1,450,603	1,400,855
2.1.	maintenance expenditure (total)	1,103,612	1,418,570	1,391,541
2.1.1.	current expenditure	1,103,612	1,418,570	1,391,541
2.2.	capital investment expenditure	36,358	32,033	9,314

Under the budget sub-programme 09.02.00 “Data protection of natural persons”, additional financial resources of EUR 50,349 were allocated to the priority action "Application of the General Data Protection Regulation and ensuring the functions assigned thereto” for 2022.

Under the budget sub-programme 09.02.00 “Data protection of natural persons” EUR 1,400,855 or 96.6% of planned expenditure were used, including for the priority action “Application of the General Data Protection Regulation and ensuring the functions assigned thereto”. In addition, funding for the audit and monitoring of the Entry/Exit Systems (ETIAS, IIS, ECRIS-TCN) within the baseline was allocated at EUR 108 224 for 2022, of which 82,096 or 75.9% were used. In 2022, own revenue from paid services amounted to EUR 7,929 or 46.8%.

32 out of 34 posts, or 94.1%, were filled in 2022, resulting in an underspending.

The use of funds and the indicators achieved in 2022 and their comparison with 2021 in the sub-programme 70.15.00 “Implementation of projects and actions under other EU policy instruments (2021-2027)” are presented in Table 2.

TABLE 2

SUB-PROGRAMME 70.10.00 "IMPLEMENTATION OF PROJECTS AND ACTIONS OF OTHER EU POLICY INSTRUMENTS (2014-2020)"

No.	Financial indicators	Previous year (actual implementation), *euro*	Reporting year, *euro*	
			approved by law	actual implementation
1.	Financial resources to cover expenditure (total)	0	44,066	44,066
1.1.	grants	0	4,840	4,840
1.3.	foreign financial assistance	0	39,226	39,226
2.	Expenditure (total)	0	44,066	8,135
2.1.	maintenance expenditure (total)	0	44,066	8,135
2.1.1.	current expenditure	0	44,066	8,135

On 31 August 2022, a contract was concluded for the implementation of the project "Distance learning programme on data protection" (project grant agreement No 101074843 – DLPDP).

The DLPDP project was submitted to the European Commission's (hereinafter – EC) financial programme "Citizens, Equality, Rights and Values" (CERV) 2021–2027 (hereinafter – CERV programme) call for proposals No CERV-2021-DATA to personal data protection supervisory authorities to enhance the target groups' knowledge of data protection rules and their implementation.

The Inspectorate is the sole implementer of the project. The project is planned to run for 48 months, from 1 September 2022 to 31 August 2024.

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

In 2022, EUR 8,135 or 18.5% of the planned EUR 44,066 were used within the DLPDP project.

The achievement of the planned results and performance indicators of the budget sub-programme 09.02.00 "Data protection of natural persons" is summarised in the table "Analysis of the achievement of results and performance indicators in 2022" are presented in Table 3.

TABLE 3

ANALYSIS OF THE ACHIEVEMENT OF RESULTS AND PERFORMANCE INDICATORS IN 2022

Name of the indicator	Planned value	Achieved result	Notes
Number of inspections on the processing of personal data	1,040	896	Given that the Inspectorate carried out a lot of public information activities, persons turn to the Inspectorate when a violation has already occurred. The number of submissions received where no data processing was detected has decreased. At the same time, while the number of inspections has decreased mathematically, their complexity has increased: they concern multiple data subjects, the processing of special categories of data (e.g. health).
Number of recommendations developed	3	3	(1) In cooperation with the Financial and Capital Market Commission and Finance Latvia, the "Recommendations for the processing of natural persons' data in the area of anti-money laundering, combating the financing of terrorism and proliferation and sanctions compliance"; (2) Recommendations on "Processing of personal data during the pre-election period" on measures to be taken when processing data of natural persons in the context of elections; (3) Recommendations for potential and current data protection officers.
Educational events (seminars, conferences, workshops) on personal data protection organised (number)	5	8	The higher score is due to the authority's proactive response to new developments and trends in data processing and protection. By organising international events, the Inspectorate increased its and the judiciary's visibility beyond national borders. (1) In accordance with the authority's work plan for 2022, six online seminars were organised for the public on current developments in the processing and protection of personal data; (2) In cooperation with the State Chancellery, participation in the 2022 LAMPA conversation festival with the erudition game "Do you know or do you think you know?"; (3) International conference "Personal Data – Future Perspective!" (three parallel sessions and six thematic blocks) with 1500 participants in person and online.
Proportion of rulings in favour of the Data State	92	93	In 2022, a total of 14 final rulings were adopted, of which one was unfavourable – in

Inspectorate in relation to the total number of court rulings (%)			an administrative offence case, based on procedural irregularities committed by the Inspectorate. In addition, 3 cases were closed on the basis of administrative agreements resulting in the withdrawal of applications.

Overall, the authority achieved the target value for the performance indicators in 2022.

12. ACTIONS PLANNED FOR 2023

1. To strengthen the Inspectorate's capacity by creating a competitive and favourable working environment and engaging professional and motivated employees in the performance of its functions.
2. To participate in the drafting of laws, regulations and development planning documents and to provide opinions on draft laws, regulations and development planning documents prepared by other institutions.
3. To publish the criteria set out in Article 41(3) of the Data Regulation on the basis of which the accreditation of supervisory bodies for codes of conduct is carried out.
4. To carry out preventive inspections on compliance with personal data protection requirements, on the activities of data controllers in the field of telemarketing, an annual supervisory inspection on credit reporting bureaus, an inspection on the use of cloud computing in the public sector, a survey of data controllers obliged to appoint a data protection officer and the completion of the Baltic States inspection on short-term vehicle rental.
5. Following the results of the preventive inspections, to make recommendations for appropriate processing of personal data in the following areas: processing of personal data using cloud computing services, and a checklist for companies (minimum data protection compliant activities).
6. To develop guidelines explaining how to carry out a data protection impact assessment.
7. To develop practical recommendations for individuals in the field of video surveillance.
8. To launch a public awareness campaign on data protection for small and medium-sized enterprises.
9. To raise public awareness of the processing and protection of personal data by organising educational seminars (at least six) and publishing explanations.
10. To complete the actions included in the SIS and VIS long-term inspection plan.
11. To fulfil the tasks set out in Sections 18 to 20 of the Data Law – to organise three examinations for data protection officers.
12. To carry out qualification maintenance testing and qualification renewal for data protection officers.
13. In cooperation with the Ombudsman's Office, to develop a clarification on the processing of personal data of State and local government officials for journalistic purposes.
14. To examine the limits of the Inspectorate's competence in matters that also fall within the remit of the police and to assess whether the Inspectorate should be given the power to block websites.