ANNUAL REPORT

of Information Commissioner for 2019

'19

Introduction by the Information Commissioner

Social developments in 2019, both in Slovenia and internationally, reveal the importance of effective protection of the right of access to public information and the protection of personal data. Concerns and challenges which lead individuals and organizations to ask the Information Commissioner for assistance further confirm the importance of these two rights. The issues brought before the Information Commissioner are diverse, but they have a common ground, namely they show how much work we still have as a society in both fields. The good news is that in Slovenia the independent supervisory authorities, including the Information Commissioner, enjoy an extremely high level of public trust, higher than the European average, as they are the first port of call for individuals who turn to them for help in case of violations. This is evidenced by the Eurobarometer survey conducted in 2019, which revealed that in Slovenia people have an above-average understanding of the General Data Protection Regulation (GDPR), individuals' rights and of the existence of a supervisory body, compared to the rest of the Europe. In comparison to the 2015 survey this share even increased considerably.

The analysis of the work of the Information Commissioner in 2019 shows a growing trend of complaints due to the non-responsiveness of the body as one of the challenges in the field of access to public information (the share of such complaints reached 44%). In the field of personal data protection and privacy, in the last two years we witnessed a significant increase in the number of reports and complaints regarding the exercise of individuals' rights. At the same time, we still face significant challenges due to the delay in adopting national rules for the implementation of the GDPR and for the transposition of the Law Enforcement Directive, to which the Information Commissioner has drawn attention for more than three years. It is particularly crucial that the legislature prevents Slovenia from being included in the list of countries that do not have properly regulated legal competences of the data protection supervisory authority.

In the area of access to public information, the number of complaints in 2019 was at a level comparable to 2018 (540 appeals were filed in 2019). The bodies with the largest share of complaints due to the non-responsiveness of the body are state bodies (ministries and constituent bodies), against which most complaints were filed due to non-responsiveness (29%). After 16 years since the Access to Public Information Act (the ZDIJZ) came into effect, these liable bodies should definitely be able to process all requests in a timely manner (within 20 working days). On the other hand, the number of complaints due to the non-responsiveness of municipal authorities decreased. 26 complaints against non-responsiveness were lodged by the media. Most commonly, these proceedings were aimed against the non-responsiveness of state bodies (10 complaints). The Information Commissioner conducted 17 proceedings against liable business entities, representing only 3% of all appeal cases.

All this shows that liable bodies do not respond in time because they do not start resolving the requests they received under the ZDIJZ in a timely manner. In the future, (even) more effort should be invested in the active training of liable bodies, which is primarily the task of the Ministry of Public Administration. The Information Commissioner, as the complaints body, may only give informal advice to the bodies based on its established practice. In 2019, the Commissioner issued 300 written responses to liable bodies and answered 629 telephone calls, while also regularly publishing cases on its website. These activities are all aimed at facilitating the work of liable bodies and informing the public about the importance of this fundamental human right. To raise awareness about the practice of the Information Commissioner, it conducted five practical workshops for administrative units. Based on the experience from 2019, the Information Commissioner calls on liable bodies to apply a narrow interpretation of the exceptions from free access to public information, taking into account the principle of partial access and documents that are absolutely public, such as data related to the employment relationship of civil servants. These principles remain unchanged even with the GDPR coming into force.

In the field of personal data protection, the Information Commissioner handled 974 complaints or requests for initiating an inspection procedure, which is the highest number of complaints thus far, and it initiated 139 minor offence procedures. Furthermore, it received 181 complaints from individuals related to the violation of the right to be informed of their own personal data, the right to be informed of their own health documentation, and the right to be informed of the health documentation by other eligible persons. At the international level, the Information Commissioner performed 148 cross-border cooperation procedures according to Articles 60 and 61 of GDPR with regard to the controllers who perform cross-border personal data processing, whereby in 77 proceedings it identified itself as the relevant supervisory authority (accord-

ing to Article 56 of GDPR). In 2019, the Information Commissioner also received nine notifications of patient data breaches on the basis of Article 46 of the Patients' Rights Act and 137 official notifications regarding personal data protection breaches on the basis on Article 33 of GDPR. The most common cases were the loss or theft of personal data storage media (e.g. personal computers and USB sticks), unauthorised access to personal data due to software errors or the abuse of power committed by employees, a hacking attack on an IT system, preventing access to data due to encryption using malicious code, and forwarding personal data to unauthorised or wrong persons. When examining complaints and performing preventive inspections, the Information Commissioner has found that the irregularities or deficiencies discovered are still largely the result of unfamiliarity with legislation or the failure to understand legislation, which is also due to the fact that the new Personal Data Protection Act (hereinafter: ZVOP-2), which would more clearly determine specific rules regarding the implementation of GDPR, has still not been adopted. Complaints and breaches of GDPR also often occur because controllers fail to provide relevant or complete information to individuals when collecting personal data; the Information Commissioner will pay additional attention to this in 2020.

Because most bodies responsible for disclosing public information do not wish to violate the legislation and want to act in compliance with the law, they need to be assisted in this and offered suitable tools, such as opinions, guidance, forms, infographics, etc. For this reason, in 2019, the Information Commissioner continued its enhanced actions for ensuring compliance, prevention, and assistance to individuals in the field of data protection as well. It provided advice to 3,284 individuals and legal entities by issuing 1,261 written opinions and answering 2,023 phone calls. Another important group of the Information Commissioner's partners in dialogue are data protection officers, of whom there are more than 2000. The Information Commissioner successfully participated in the European Commission's calls for applications for projects from the REC Programme (Rights, Equality and Citizenship Programme) with the goal of additionally strengthening all of these activities.

With regard to other mechanisms arising from GDPR related to the accountability principle, the Information Commissioner assesses that the knowledge concerning the performance of impact assessments connected to personal data protection, which are significant for ensuring the responsible introduction of risky forms of processing and new technologies for personal data processing, is improving. This should also be a key component in the procedure for drafting new regulations that foresee serious intrusions into the privacy of individuals and/or the introduction of modern technologies.

The experience from 2019 also indicated numerous challenges at the level of the European Union (EU) and in cooperation within the European Data Protection Board (EDPB), especially when it comes to performing cross-border procedures and differences in national procedural rules in EU Member States. This is also one of the reasons for these procedures being longer and the first decisions being expected no earlier than in 2020. On the one hand, answers are sought by the EDPB, which is actively seeking common definitions and interpretations of the concepts from GDPR, while on the other hand, the European legislature can also help resolve this issue, particularly by considering a potential future audit of GDPR.

The challenges that we will face in both areas are also not insignificant in 2020, but I believe that the Information Commissioner will be able to continue tackling them with its skilled and experienced team, constructive cooperation with all stakeholders, and openness to individuals and organisations. In any case, however, it is the legislature that holds great responsibility in the field of data protection, as what happens with data protection in Slovenia in the future depends on the legislation.

Mojca Prelesnik, Information Commissioner

THE INFORMATION COMMISSIONER

THE ESTABLISHMENT OF THE INFORMATION COMMISSIONER AND ESSENTIAL INFORMATION

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act (Official Gazette RS, Nos. 113/05 and 51/07 – ZUstS-A, hereinafter: the ZInfP), establishing a new and independent state authority as of 31 December 2005. The Act combined two authorities, namely the Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection. Upon the entry into force of the ZInfP, the Commissioner for Access to Public Information continued the work as the Information Commissioner and took over the inspectors and other staff of the Inspectorate for the Protection of Personal Data, its equipment and assets. At the same time, it took over all pending cases, archives and records kept by the Inspectorate for the Protection of Personal Data. Thus, the scope of the body responsible for the implementation of the right to access public information changed significantly and expanded to the field of personal data protection. The Information Commissioner thus also became the national supervisory authority for data protection. It commenced its work on 1 January 2006.

Mojca Prelesnik is the head of the Information Commissioner as of 17 July 2014.

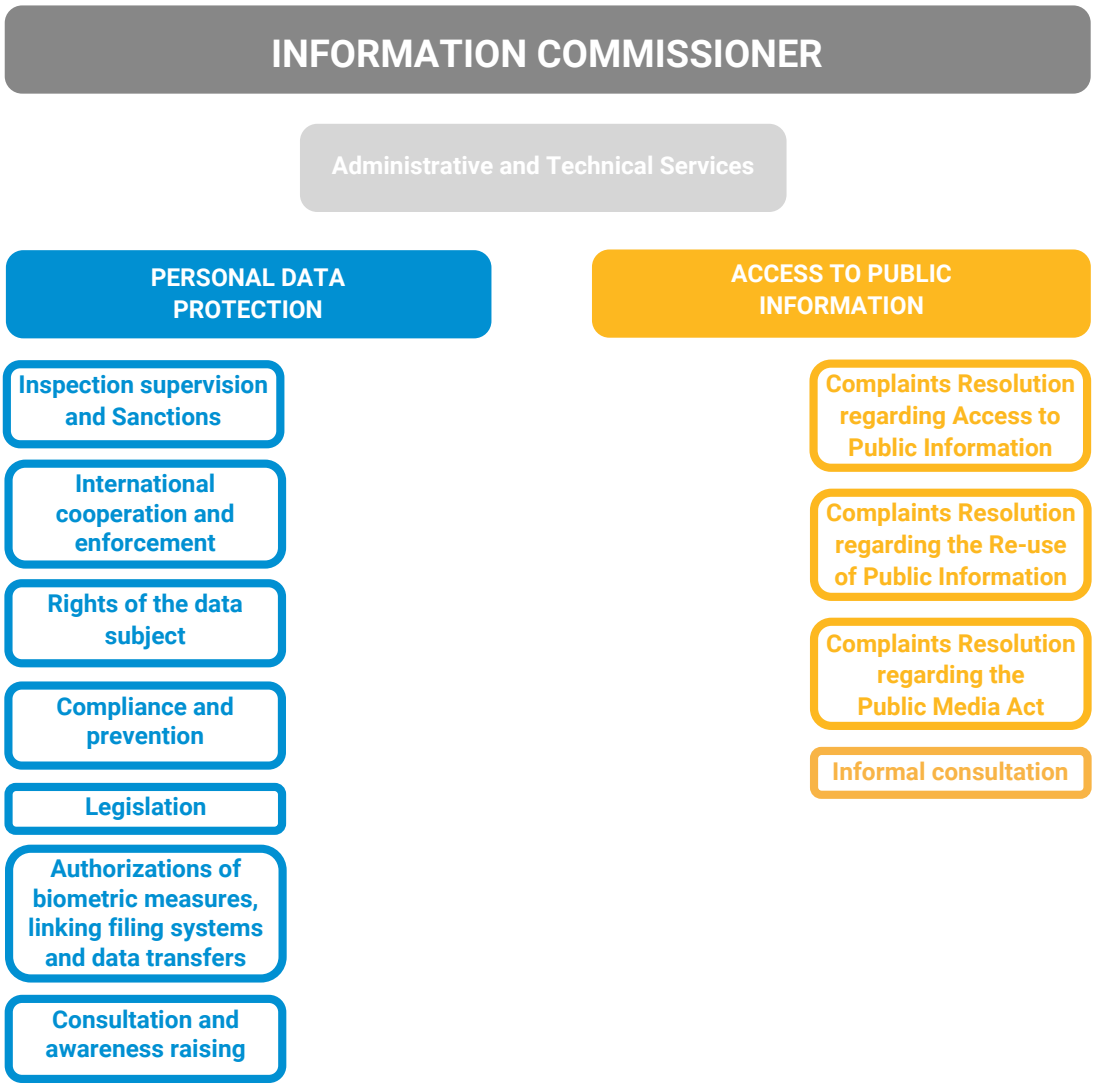
ADDRESS
Republic of Slovenia
Information Commissioner
Dunajska cesta 22
1000 Ljubljana

CONTACT
Telephone: 01 230 97 30
Fax: 01 230 97 78
E-mail: gp.ip@ip-rs.si
WEBSITE www.ip-rs.si

DATA PROTECTION OFFICER dpo@ip-rs.si
REPORTING DATA BREACH prijava-krsitev@ip-rs.si

Organisational Structure

The Information Commissioner carries out its tasks through the following organisational units:
- The Secretariat of the Information Commissioner;
- The Public Information Sector;
- The Personal Data Protection Sector;
- Administrative and Technical Services.



Organisational Chart of the Information Commissioner.

At the end of 2019, the Information Commissioner had 47 employees, of which one was employed on the basis of a temporary contract.

KEY AREAS OF PERFORMANCE AND MAIN COMPETENCES

KEY AREAS OF PERFORMANCE AND MAIN COMPETENCES

The Information Commissioner performs its statutory tasks and competences in two fields:
- In the field of access to public information;
- In the field of data protection.

In accordance with Article 2 of the ZInfP, the Information Commissioner is competent to:
- Decide on appeals against a decision by which an authority denied or refused the applicant's request for access or in any other manner violated the right to access or re-use public information, and also, within the frame of complaints procedure, supervise the implementation of the act regulating access to public information and regulations adopted thereunder (as the appellate authority in the area of access to public information);
- Perform inspections regarding the implementation of the Act and other regulations governing the protection or processing of personal data or the transfer of personal data out of the Republic of Slovenia, as well as perform other duties determined by these regulations;
- Decide on appeals of individuals against the refusal of a data controller to grant the request of the individual with regard to his right to access the requested data, and to extracts, lists, viewings, certificates, information, explanations, transcripts, or copies in accordance with the provisions of the act governing personal data protection;
- File a request before the Constitutional Court of the Republic of Slovenia for the review of the constitutionality of a law, regulation, or general act issued for the exercise of public authority if a question of constitutionality or legality arises in connection with proceedings it is conducting, in both the field of access to public information and personal data protection.

The entry into force of the General Data Protection Regulation had an immense impact on the work of the Information Commissioner in the field of personal data protection in 2019. The GDPR is directly applicable in all EU Member States as of 25 May 2018. The Regulation requires the adoption of a new Personal Data Protection Act (ZVOP-2), implementing the GDPR in the Republic of Slovenia; however, such an act was not adopted by the end of 2019. Therefore, in addition to the GDPR, ZVOP-1 is still applicable, namely the provisions of the act which are not regulated by the GDPR and which do not contradict it.

In the area of access to public information, the Information Commissioner also has competences determined by the Mass Media Act (Article 45, hereinafter: the ZMed). A liable authority's refusal of a request by a representative of the media shall be deemed a decision refusing the request. The authority competent to decide on appeals is the Information Commissioner.

The Information Commissioner is also responsible for managing the record of all exclusive rights granted in the field of re-use of information (Article 36a, Paragraph 5 of ZDIJZ).

The Information Commissioner is competent under the Patients' Rights Act (ZPacP), the Travel Documents Act (ZPLD-1), the Identity Card Act (ZOIzk), Electronic Communications Act (ZEKom-1), Central Credit Register Act (ZCKR), Consumer Credit Act (ZPotK-2), Decree on unmanned aircraft systems and Decree on the implementation of the Regulation (EU) on citizens' initiative.

With the entry of the Republic of Slovenia into the Schengen Area, the Information Commissioner also assumed responsibility for supervision of the implementation of Article 128 of the Convention Implementing the Schengen Agreement and is thus an independent body responsible for supervising the transfer of personal data for the purposes of the mentioned Convention.

FINANCIAL MANAGEMENT IN 2019

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the proposal of the Information Commissioner (Article 5 of the ZInfP).

In the fiscal year 2019, the operating budget of the Information Commissioner amounted to EUR 2,232,236.00, of which EUR 1,871,937.00 were spent on wages and salaries, EUR 346,447.00 on material costs and expenses and EUR 13,852.00 on investments. Material costs and expenses were necessary for the normal functioning of the Information Commissioner (stationery, travel expenses, cleaning expenses, student work payments, postal services, the education of employees, producing brochures, etc.).

2 ACCESS TO PUBLIC INFORMATION – IN THE NAME OF THE PEOPLE AND FOR THE PEOPLE

2.1 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

The right to access public information was already granted by the legislature in the Constitution of the Republic of Slovenia. The second paragraph of Article 39 of the Constitution determines that everyone has the right to obtain information of a public nature in which they have a well founded legal interest under law, except in such cases as are provided by law. This right is further regulated in the Access to Public Information Act (hereinafter: the ZDIJZ). The bodies liable under the ZDIJZ are divided into two groups:

- Bodies, i.e. State bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors;
- Liable business entities subject to dominant influence of entities of public law.

The liable bodies are obliged to provide public information in two ways: by publishing it on the Internet and by providing access upon individual requests.

The ZDIJZ provides the right to access information that has already been created and exists in any form. Thus, this act provides for the transparency of the use of public money and the decisions of the public administration, which should work on behalf of the people and for the people.

In 2019, the Information Commissioner received 540 appeals, of which 305 were against decisions refusing requests (17 of those appeals were against liable business entities subject to dominant influence of entities of public law), while 235 were against the non-responsiveness of first-instance authorities.

In appeal procedures the Information Commissioner issued 301 decisions on the merits, while in two cases it rejected the appeal. In processing the appeals of individuals, 42 so-called in camera examinations were carried out.

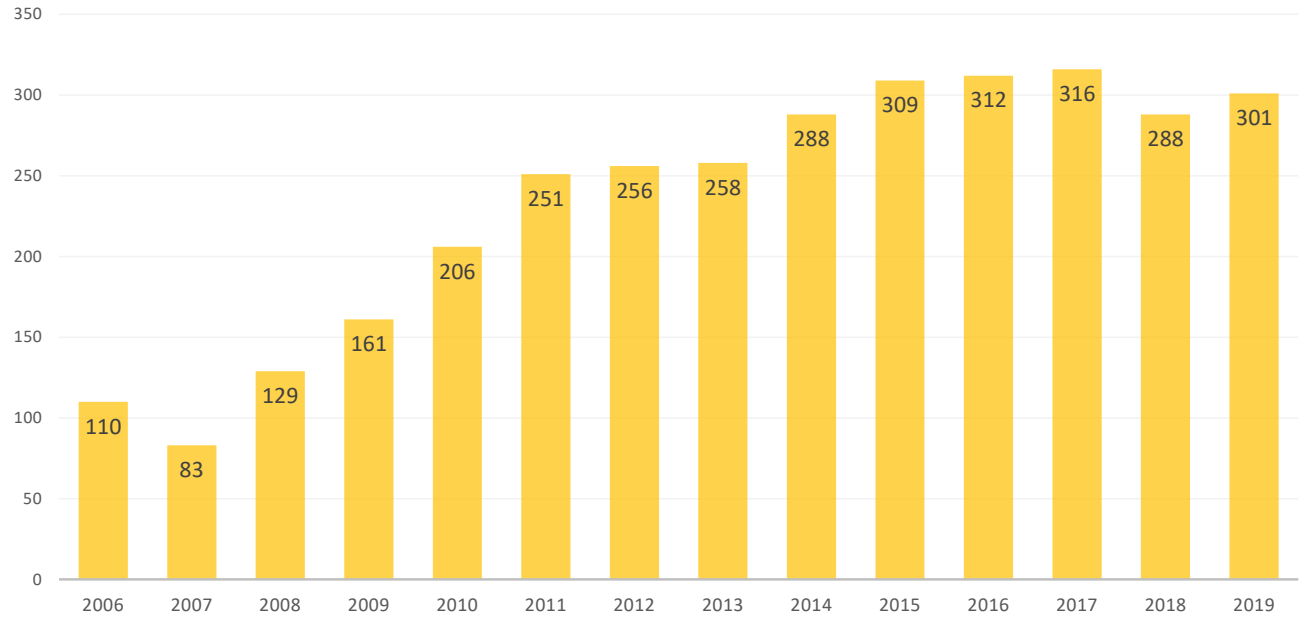
The Information Commissioner received 235 appeals against the non-responsiveness of the authorities. The Information Commissioner first called on the liable authorities to decide on the requests as soon as possible, which in most cases they did. In 28 cases the Information Commissioner rejected the appeal (in 23 of those cases because the appeal was lodged too soon and in 5 cases because the application was incomplete), in 15 cases it issued the explanation that it was not competent to consider their applications and advised the individuals how to act. 19 applicants withdrew their appeals as they received the requested documents.

In 2019, the Information Commissioner received 300 written requests for assistance and various questions of individuals regarding access to public information. During business hours the Commissioner also answered 629 telephone calls about questions from the field of access to public information. The Information Commissioner replied to all applications to the extent to which it is competent, and in most instances it referred them to the competent institution – The Ministry of Public Administration.

The following actions were taken amongst the (301) decisions issued by the Information Commissioner:

- In 136 cases it dismissed the appeal;
- In 114 cases it partially or fully granted the appeal of the applicant or decided in favour of the applicant;
- In 48 cases it granted the appeal and returned the matter to the first instance body for reconsideration;
- In 2 cases it rejected the appeal;
- In 1 case it declared the first instance decision null.

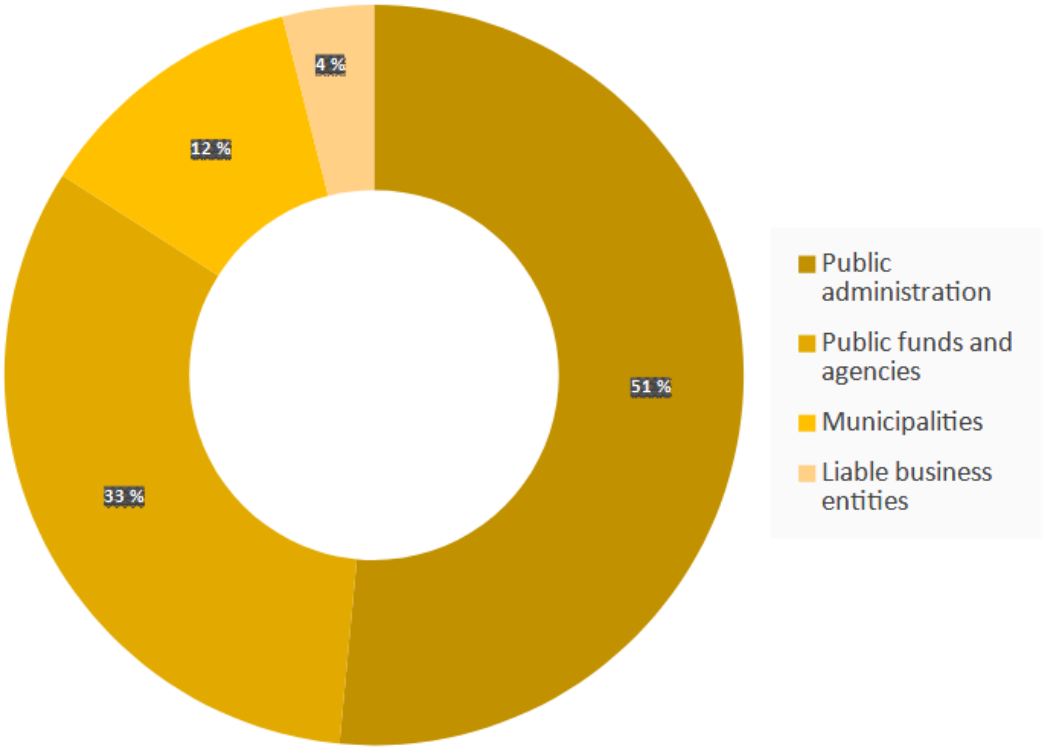
The number of decisions issued in relation to access to public information from 2006 to 2019



The following categories of liable bodies were subject to the Information Commissioner's decisions in the appeal process, as they refused access to public information:

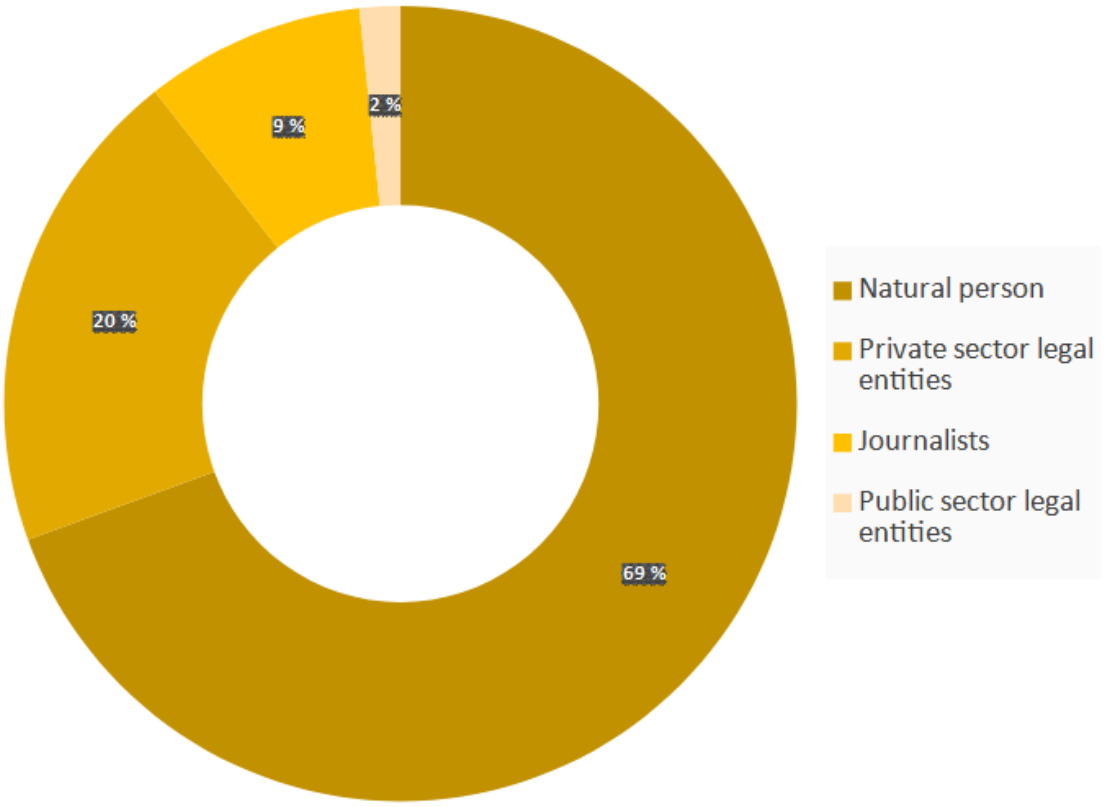
- Public administration (ministries, constituent bodies, public administration units) (155 cases);
- Public funds, institutes, agencies, public service contractors, and holders of public authority (98 cases);
- Municipalities (36);
- Liable business entities subject to dominant influence of the state, municipalities and other public law entities (12).

Categories of bodies liable subject to appeal.



In 209 cases applications were submitted by natural persons, in 60 cases complaints were submitted by private sector legal entities. 27 complaints were submitted by journalists and 5 by public sector legal entities.

Categories of applicants who appeal the refusal of access to public information.



In 2019, 34 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 11.3 % of the decisions issued). The relatively small portion of such appeals indicates a greater level of transparency and openness in the public sector in relation to its operations and the acceptance of the Information Commissioner's decisions by various authorities and applicants.

In 2019, the Administrative Court issued 52 judgments in relation to appeals filed against the decisions of the Information Commissioner. In 23 cases, the Court dismissed the appeal, in 20 cases the Court granted the appeal and returned the matter to the Information Commissioner for reconsideration, in 5 cases it issued a decision rejecting the appeal, in 3 cases it issued a decision staying the procedure and in 1 case the Court decided partially in favour of the appellant and partially dismissed the appeal.

2.3 SELECTED CASES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

The names and surnames of the holders of diplomatic passports are not protected personal data

The applicant requested, from the Ministry of Foreign Affairs of the Republic of Slovenia, all documents relating to the diplomatic passports of four representatives of the Catholic Church. The body partially refused the application by invoking the right to personal data protection according to point three of paragraph one of Article 6 of the Access to Public Information Act (ZDIJZ). It provided the applicant with the requested documents, whereby the names and surnames, dates of birth, titles, addresses, e-mails, phone numbers, signatures, and other data on the basis of which the identity of the holders of diplomatic passports could be inferred had been redacted. It found that there was no public interest. Pursuant to the provision of Article 44 of the General Administrative Procedure Act (ZUP), the Information Commissioner invited all four persons to whom the request for public information referred to intervene in the appellate procedure. None of the invited individuals expressed their intention to intervene prior to the issuing of the decision. Because personal data means any information relating to an identified or identifiable natural person ('data subject'), whereby an identifiable natural person is one who can be directly or indirectly identified, it was not disputed in the matter at hand that all of the requested documents contain personal data of four specific natural persons and that they meet the criteria for an exception from free access according to point three of paragraph one of Article 6 of the ZDIJZ. As a general rule, it arises from the GDPR that personal data processing (i.e. the disclosure of data to the public) is lawful (permissible) when processing is necessary for compliance with a legal obligation to which the controller is subject (point c) or when processing is necessary in the exercise of official authority vested in the controller (point e). Such legal basis for personal data processing in the procedure with a request for access according to the ZDIJZ, taking into account Article 6(1)(c) of the GDPR, can also be provided by the provision of paragraph two of Article 6 of the ZDIJZ. This provision states that, without prejudice to the provisions in the preceding paragraph (exceptions from free access to public information; note by the Information Commissioner), access to the requested information is sustained if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information, except in the cases subsequently listed, which do not, however, include an exception from personal data protection. When performing the prevailing public interest test, the Information Commissioner based its presumptions on the finding that the applicant requested the documents that had been drafted in the procedures for issuing diplomatic passports on the basis of national interest after four specific individuals submitted an application (request) for the issuance of such passports. This national interest is assessed in accordance with the Regulation, which specifies in greater detail the criteria for determining the interest of the Republic of Slovenia on the basis of which a diplomatic passport is issued; these criteria are then applied by the minister responsible for foreign affairs. As is evident from the Regulation, "when assessing the issuing of a diplomatic passport for representing Slovenia abroad, it is specifically taken into account whether the person /.../ enjoys a special reputation in any of the religious communities generally recognised internationally and historically connected with the Slovenian people or holds a high position in such a community." Therefore, the Information Commissioner has recognised that there is public interest in disclosing specific personal data of the four specific individuals and that it is in the legitimate interest of the public to discover in what way the state performs the policy of issuing diplomatic passports on the basis of national interest, what or who it deems to be an eligible holder of a diplomatic passport issued on the basis of national interest when it is needed for representing Slovenia abroad, and who enjoys a special reputation in a generally internationally recognised religious community which is historically connected with the Slovenian people or holding a high position in such a community. When granting a diplomatic passport on the basis of national interest, a person is given such a passport within the procedure for discovering such interest, and the decision-making regarding its existence is at the discretion of the minister responsible for foreign affairs. According to the Information Commissioner, it is in such cases that it is important that specific information is also publicly accessible from the perspective of understanding the consequences of the decisions made in the public sector. This way, citizens are able to understand the consequences of the decisions made by public authorities and they can express any (essential) reservations regarding such decisions. The transparency of the work of public office holders and officials also reduces the possibility of irresponsibly adopting political and expert decisions. The transparency of their work contributes to more informed decisions and, as a result, to raising the quality of performing public services and of specific procedures carried out by authorities, and to reducing corruption risks. Because it is evident from the legal definition (paragraph one of Article 9 of the Travel Documents Act – ZPLD-1) that the issuing of diplomatic passports to specific individuals must be in the interest of the Republic of Slovenia (and not in their personal interest), it is deemed by the Information Commissioner that their right to personal data protection relating

to their names and surnames must be subordinate to the public interest which prevails in this case. Taking into account the principle of data minimisation (point c) of Article 5 of the GDPR, there is no free access to the personal data that is not essentially connected with the granting of the diplomatic passport, i.e. date and place of birth, residence, and e-mail.

KEY TERMS: personal data, Decision No 090-285/2018.

The sections of the document referring to the use of public funds are not a trade secret

The applicant (journalist) requested that Slovenian Sovereign Holding provides the agreement on the termination of employment with the chairwoman of the board. The authority dismissed the request by the applicant by referring to the exception of protecting trade secrets according to point two of paragraph one of Article 6 of the Access to Public Information Act (hereinafter: the ZDIJZ). The applicant filed an appeal against the decision, as they believed that the data concerning the amount of funds or other compensation to the chairwoman of the board on the basis of the agreement on the early termination of employment was in the absolute interest of the public. In the appeal procedure, the Information Commissioner found that the criterion regarding trade secrets according to paragraph one of Article 39 of the Companies Act (hereinafter: the ZGD-1) had been met concerning the requested agreement. This criterion sets forth that a trade secret is any data classified as trade secret by the company by way of a written decision; and that company members, employees, members of company bodies, and other persons who must protect trade secrets must be informed of this decision. Although the requested agreement was classified as trade secret by the holding based on subjective criterion, the Information Commissioner found that the requested information is considered to be data that, according to paragraph three of Article 39 of the ZGD-1, cannot be defined as a trade secret. The agreement contained information that is public by law, namely according to indent one of paragraph three of Article 6 of the ZDIJZ. According to this Article, notwithstanding the provisions of paragraph one of Article 6 of the ZDIJZ (i.e. regardless of the exception for a trade secret), the access to the requested information is permitted if this is information concerning the use of public funds, with the exception of cases arising from points 1 and 5–8 of paragraph one of Article 6 of the ZDIJZ or cases in which the act governing public finances or the act governing public procurement stipulate otherwise. Although the ZDIJZ does not contain a definition of public funds, this definition has been formed for the purposes of access to public information through the practice of the Information Commissioner and the case law of the courts. The concept of the use of public funds (according to e.g. the judgment of the Administrative Court I U 764/2015-27 of 24 August 2016) is defined as any use of assets, for or without consideration, including any change or transformation of assets from one form to another; therefore, the use of public funds is not only the outflow of assets from the account of a public institution, but also all other forms of using public funds, for or without consideration. It is, therefore, clear from the public nature of the organisation, from tasks for the fulfilment of which the authority was founded, and from the origin or the holding of the assets managed by the authority, that the authority has at its disposal and manages public funds and that any disposal of public funds (including in the event of payments or commitments to disburse public funds) is public. For this reason, the Information Commissioner ordered that the authority provides those parts of the requested document to the applicant which show the reasons, conditions, and amounts of the disbursements of public funds.

KEY TERMS: trade secret, the media, Decision No 090-130/2019

The unique identification number of a state prosecutor is information related to the performance of public office

The applicant requested that the Supreme State Prosecutor's Office of the Republic of Slovenia provides the electronic records of all special statistical sections of the annual reports of all state prosecutor's offices, which had been drafted and submitted prior to the submission of the request in accordance with the Rules in the form of an annual report on the operation of the state prosecutor's office. The Office refused the applicant's request to access the 'unique identification (ID) number of a state prosecutor' and the 'unique ID number of a criminal offence' by referring to the exception of personal data protection and the protection of criminal proceedings. It stated that, by connecting the ID of the state prosecutor and the ID of a criminal offence, personal data relating to a specific individual could be deducted, which would lead to the direct or indirect identification of a specific state prosecutor. Connecting both of the IDs could result in disclosing the identity of the competent state prosecutor handling a specific criminal offence in the phase in which such

a disclosure could harm the interests of the criminal proceedings, as the requested information, if further researched, without great effort, also enables the identification of a specific criminal matter. The applicant filed an appeal against the decision of the Office, as it found that the state prosecutor's ID is not their protected personal data, but merely information regarding the performance of public office, which discloses that a particular state prosecutor has performed some procedural actions and what the scope of their work was. The Information Commissioner found in the appeal procedure that the processing of personal data is lawful if one of the legal foundations stipulated by paragraph one of Article 6 of GDPR is met. As a general rule, it arises from this Article that personal data processing (i.e. also the disclosure of data to the public) is also lawful (permissible) when processing is necessary for the compliance with a legal obligation to which the controller is subject (point c)) or when processing is necessary in the exercise of official authority vested in the controller (point e)). Such legal foundation for personal data processing in the procedure with a request for access according to the ZDIJZ, taking into account point c) of Article 6(1) of GDPR, can also be provided by the provision of indent 1 of paragraph three of Article 6 of the ZDIJZ. According to this provision, access to the requested information shall be permitted if this is information related to the use of public funds or information related to the execution of public functions or employment relationship of the civil servant, with the exception of cases arising from points 1 and 5–8 of paragraph one or cases in which the act governing public finances or the act governing public procurement stipulate otherwise. It is therefore undisputed that the case arising from point 3 of paragraph one of Article 6 of the ZDIJZ (personal data protection) is not among the statutory exceptions that would be exempt from the obligation of the Office to provide the requested information if they are related to the execution of public functions or employment relationship of the civil servant. The information regarding the unique identification number of a state prosecutor refers to an individual state prosecutor and represents their anonymous code (Article 13 of the Rules) allocated to the state prosecutor for the purposes of performing tasks under their purview; for this reason, the Information Commissioner found that this was information related to the execution of their public function. Conceptually, the information regarding the unique identification number of a criminal offence cannot be deemed personal data, as this is the unique code of a criminal offence. The Office also failed to show that there is an exception according to point 6 of paragraph one of Article 6 of the ZDIJZ. In order to successfully invoke grounds for the exception of protecting criminal proceedings, two conditions must be met cumulatively: (1) the requested information has been acquired or drawn up for the purposes of criminal prosecution or in connection therewith and (2) the disclosure of the requested information would prejudice the implementation of such procedure. According to the provision of point 6 of paragraph one of Article 6 of the ZDIJZ that access may only be refused if the data refers to specific criminal proceedings that are still ongoing. This provision cannot be interpreted so broadly as to also enable the enforcement of this exception in the event of future ("re-opened") criminal prosecutions, whereby the Information Commissioner agreed with the position of the applicant that, by way of such a broad interpretation, the Office could conceal all information regarding prosecution until the statute of limitations for the criminal prosecution expires. Because the ID number of a state prosecutor is not protected personal data and because the Office failed to show that the condition of damage to the proceedings has been met, and thus the ID number of the criminal offences could be redacted, the Information Commissioner ordered the Office to provide the requested data.

KEY TERMS: criminal proceedings, personal data, Decision No 090-3/2019

Data on which products have been delivered and at which price is information on the use of public funds

The applicant requested that the Faculty of Medicine in Ljubljana provide a photocopy of the tender pro forma invoice enclosed by the selected bidder in the public procurement procedure. The Faculty rejected the section of the applicant's request referring to the column 'Name, manufacturer, and the brand of the goods subject to this tender procedure' by invoking an exception due to a trade secret. This was also claimed by an intervener who was invited by the Faculty into the procedure. The applicant filed an appeal against the decision, because, up to the moment when the Faculty invited the intervener into the procedure, none of the parts of the bid had been labelled as a trade secret and no decisions regarding this had been attached to the bid. Furthermore, this data needs to be disclosed pursuant to paragraph three of Article 6 of the ZDIJZ (use of public funds), and the information regarding the goods subject to the bid is also public pursuant to paragraph two of Article 35 of the Public Procurement Act (ZJN-3). The Information Commissioner sought to discover within the appeal procedure whether the requested information was actually an exception according to point 2 of paragraph one of Article 6 of the ZDIJZ, as was claimed by the intervener in the first-instance proceedings. Because the matter referred to a document which had been submitted to the Faculty by the intervener as part of their bid within the public procurement procedure on

25 May 2018, i.e. before the Trade Secrets Act (ZPosS) entered into force, the Information Commissioner took into account the provisions of Articles 39 and 40 of the ZGD-1, which had been in force before the ZPosS entered into force. The ZGD-1 distinguishes two criteria for determining a trade secret, namely the subjective (paragraph one of Article 39 of the ZGD-1) and the objective criteria (paragraph 2 of Article 39 of the ZGD-1), depending on what grounds data is considered to be a trade secret. Data that is public by law or data regarding a violation of a law or best business practice (paragraph three of Article 39 of the ZGD-1) cannot be designated as a trade secret. With the subjective criterion, the company itself, by way of a general or individual act, order, etc., designates specific data as confidential, regardless of what significance it holds for its competitive advantage (this could also be less important data), what kind of damage would be incurred by way of disclosure, if any, etc. The decision on whether particular data will be designated as a trade secret according to paragraph one of Article 39 of the ZGD-1 is therefore entirely in the hands of the company. Because the case law regarding the timeliness of issuing a decision establishing a trade secret is clear, the submitted decision on designating a trade secret of 31 May 2019 cannot be considered timely and was not relevant for examining the specific appeal procedure. A decision may be used to designate information as a trade secret retroactively as well, but such a decision is only timely if issued prior to receiving a request to access public information (see judgments no. U 1976/2008 of 26 May 2010, no. I U 599/2014 of 3 November 2015, no. I U 1573/2014 of 18 November 2015). The content of the information and the evident serious consequences of its disclosure are determining factors in designating specific data as a trade secret according to paragraph two of Article 39 of the ZGD-1. Because a company usually has all of the necessary knowledge and experience in the market in which it operates and it knows precisely what, how, and why something could impact its competitive advantage, merely general, abstract, and unfounded invocation of a trade secret does not suffice (see judgments no. U 284/2008 of 27 May 2009, U 1276/2008 of 11 February 2010, I U 1132/2015 of 27 January 2016). Because the auxiliary participant failed to clarify why the requested information constituted a competitive advantage, which must be protected as a trade secret, the objective criterion for a trade secret was also not met in this case. Because paragraph three of Article 39 of the ZGD-1 stipulates that no data which is public by law can be designated as a trade secret, the bidders and contracting authorities must be aware on the basis of the law itself that complete protection of the trade secret in the documents obtained or drafted on the basis of a public procurement procedure cannot be expected. The basic principles of the ZJN-3 (Articles 3 - 8) ensure that public contracts are public to the general public as well as to special public groups (e.g. to the unsuccessful bidders in a public procurement procedure) and they also provide control over the proper functioning of the public sector, which prevents poor management, abuse of power, and corruption. The Information Commissioner found that the principle of public disclosure also covers the information on the 'name of the goods subject to the bid' and 'manufacturer or trademark'. The information regarding the name of the goods subject to the bid falls within the framework of the 'specifications for the goods subject to the bid', which are, according to paragraph two of Article 35 of the ZJN-3, public information. The term 'specification' is completely clear. A 'specification' is defined as: "a detailed description or designation of something depending on its special, distinctive properties", which clearly shows that a specification not only defines the subject of the public contract using 'basic' data, but all data regarding the subject of the public contract that is so significant for the contracting authority that it was specifically defined in the tender documents. This means that the scope of the information within the framework of the 'specifications for the goods subject to the bid' always depends on the requirements of the contracting authority – who defines them in the tender documents. As a result, the bidder must indicate in their bid that the subject of the bid meets all (and not just some) requirements from the specification, otherwise they will be eliminated from the procedure. The data regarding the manufacturer of the goods or the brand indicate information on the subject of the public contract, which means that this is data on the use of public funds in accordance with indent one of paragraph three of Article 6 of the ZDIJZ. The information deals with what (which products) the Faculty purchased using public funds. Therefore, the Information Commissioner dismissed the contested decision and ordered the Faculty to provide the requested data.

KEY TERMS: public contracts, Decision No 090-153/2019

2.6 AWARENESS RAISING ACTIVITIES

The Information Commissioner performs a variety of activities for raising awareness of both the specialised and general public. Among other activities, it organizes a yearly event to celebrate the **Right to Know Day**. Within the scope of the events held to observe World Right to Know Day, the Information Commissioner organised a panel titled 'Challenges and Solutions in the Procedure for Accessing Public Information', where discussions dealt with both procedural and substantive dilemmas regarding the implementation of the ZDIJZ, as well as with how to tackle the challenges that liable bodies and applicants face in practice. The participants of the panel were first welcomed by Minister of Public Administration Rudi Medved and Information Commissioner Mojca Prelesnik, who stressed that the liable bodies are generally well-informed about the provisions of the ZDIJZ and have been increasingly asking the Information Commissioner for opinions and clarifications, which shows that they are active and responsive. The same also applies to all applicants, which is indicated by a constant upward trend in complaints.

In the framework of **international cooperation**, the Information Commissioner delivers lectures, publishes papers and participates in workshops, thereby maintaining contacts with foreign countries and other supervisory authorities for access to public information.

2.7 GENERAL ASSESSMENT AND RECOMMENDATIONS

The Information Commissioner finds that, in 2019, the number of complaints in the field of accessing public information is comparable to the number in 2018 (540 complaints were filed in 2019). The number of complaints against the administrative silence of public authorities increased (in 2018, the Information Commissioner examined 213 such complaints and 222 in 2019), while the number of complaints against the administrative silence of municipalities decreased (in 2018, the Information Commissioner examined 123 such complaints and 106 in 2019).

As the number of complaints against the administrative silence of public authorities has been increasing in recent years, the Information Commissioner analysed these complaint procedures in greater detail. It was discovered that a complaint procedure was initiated in only 172 of the 235 complaints received due to administrative silence, while in the remaining cases the applicant's complaint was premature, incomplete, or the issue was not the administrative silence of a body liable for disclosing public information according to the ZDIJZ, because the request had not been given according to the said Act. In the 172 cases in which the Information Commissioner initiated a complaint procedure against the bodies liable for disclosing public information, the vast majority of these bodies eliminated their administrative silence after an additional deadline and fully or partially enabled the applicants to gain access to the requested information (in 130 cases), while in 42 cases these bodies issued a decision of rejection and dismissed the requests. Of all of the received complaints against the administrative silence of a public body, 26 were filed by the media because they had not received the requested information within seven business days as stipulated in Article 45 of the Mass Media Act (ZMed). In these cases, the largest group of the complaints received by the Information Commissioner were once again complaints against public administration authorities (10 complaints).

This indicates that the liable bodies are generally not silent because they do not wish to provide the requested information, but the Information Commissioner finds that they fail to begin resolving requests according to the ZDIJZ in a timely manner and, as a result, they miss the final statutory deadline for a decision. According to the statistics, we found that approximately 30% of the complaints filed due to administrative silence are unfounded, but it is still concerning that the number of complaints received against public administration authorities (ministries and their bodies) is increasing. It is against these liable bodies that the largest proportion of complaints was filed due to administrative silence (29%), namely against the public administration in its narrow definition, which should, after 16 years of the ZDIJZ being in force, certainly be able to examine all requests for access to public information in a timely manner, i.e. in the statutory deadline of 20 business days.

Considering the large proportion of complaints due to administrative silence in the total number of complaints (44%), the Information Commissioner finds that, in the future, (even) more efforts will have to be made to actively train the liable bodies to apply the Act in practice, which is primarily the task of the Ministry of Public Administration, which, according to Article 32 of the ZDIJZ, advises these bodies regarding the

application of this Act and performs promotional and development tasks. The Information Commissioner, as the appellate body, can only advise liable bodies within the scope of informal consultation, on the basis of cases from practice that have already been examined. In 2019, the Information Commissioner provided 300 written answers to questions sent by these bodies and provided advice through a telephone on-call service 629 times. With the purpose of introducing its practice, it also carried out five practical workshops for administrative units, with 134 participants from 51 administrative units participating. The Information Commissioner regularly posts its practical cases on its website, making an effort to keep them up-to-date and clearly visible, with the purpose of facilitating the work of the liable bodies and informing the public of the significance of this fundamental human right.

In 2019, the Information Commissioner conducted 17 procedures against business entities subject to dominant influence, which accounted for only 3% of all complaints. The Information Commissioner found that the number of these complaints has remained low throughout the years.

On the basis of specific complaint cases, the Information Commissioner provided the following findings and recommendations for the future work of the bodies liable for disclosing public information:

- In 2019, as in 2018, the Information Commissioner detected an increase in the number of complaint procedures regarding the access to information referring to civil servants and public officials (the number of complaints received increased by 75%). Because, in these cases, the liable bodies refused access to the requested information without just cause by referring to protected personal data, the Information Commissioner warns that, even after GDPR was implemented, this data is still designated as absolutely public in accordance with paragraph three of Article 6 of the ZDIJZ. This is also the long-term practice of the Information Commissioner and the Administrative Court.
- In 2019, the Information Commissioner once again detected an increase in the number of complaints that refer to documents arising from inspection procedures. In these complaint procedures, it was found that the liable bodies often failed to apply the partial access rule without just cause, but rather fully refused access to applicants, even though the requested information did not meet statutory exceptions to freely accessible information. It should be noted that, if a document, or a part thereof, only partially includes protected information and this information can be excluded from this document without putting its confidentiality at risk, the body must follow the partial access rule and inform the applicant of the content of the unprotected part of the document.
- Because the liable bodies must also provide information to the public themselves, without a request from an applicant, the Information Commissioner is asking them to pay more attention to this and to act proactively, so that they may avoid potential procedures according to the ZDIJZ. The Information Commissioner found in multiple complaint procedures in 2019 that the subject of the request was information that the bodies should have published themselves according to Articles 10 and 10.a of the ZDIJZ.
- In 2019, as in 2018, the Information Commissioner found that the liable bodies do not pay sufficient attention to procedural issues, and it is the result of the incompletely or erroneously determined facts of the case by the body at the first instance that the challenged decision cannot be subject to judicial review. In cases when these bodies refuse the applicant's request due to the existence of statutory exceptions, it is key that the facts of the case be fully determined and that the bodies share their specific position regarding the content of the documents requested. It must be evident from the explanatory note which documents were subject to the decision and regarding which part of these documents the applicant's request was refused. The reasons why the access to the requested documents is refused must be explained in a manner that is comprehensible to the applicants and compliant with the operative part of the decision.
- Because, in 2019, the Information Commissioner detected an increase in the number of complaints due to the administrative silence of the bodies within the public administration in its narrow definition, it is exhorting them to pay more attention to the access to public information, thus enabling that applicants' requests are examined within statutory deadlines.

3 PERSONAL DATA PROTECTION – PROTECTING THE BASIC HUMAN RIGHT TO PRIVACY

3.1 THE CONCEPT OF PERSONAL DATA PROTECTION

In the Republic of Slovenia, the concept of personal data protection is based on the provisions determined by Article 38 of the Constitution, according to which personal data protection is among the constitutionally guaranteed human rights and fundamental freedoms.

The constitutional basis for the normative regulation of personal data protection is found in the second paragraph of Article 38 of the Constitution of the Republic of Slovenia, which stipulates that the collection, processing, designated use, supervision, and protection of the confidentiality of personal data shall be provided by law (namely by a general, organic law and sectoral laws). Up to 25 May 2018 the key organic law regulating the protection of personal data was the Personal Data Protection Act (ZVOP-1).

The development of modern information and communication technologies brought about the need to adapt and update the legislative framework at the European level. On 5 May 2016, the key building blocks of the new EU legislative package on personal data protection were published in the Official Journal of the European Union, namely the General Data Protection Regulation (the GDPR) and Directive (EU) 2016/680 (the so-called Police Directive). The GDPR entered into force on 25 May 2016 and became applicable on 25 May 2018. The period for transposition of Directive (EU) 2016/680 into national law was two years.

The GDPR requires the adoption of a new organic data protection law in the Republic of Slovenia, which had not yet been adopted by the end of 2019.

3.2 INSPECTION SUPERVISION IN 2019

Due to the suspicion of violations of the provisions of the GDPR/ZVOP-1, in 2019 the Information Commissioner conducted 1,183 cases of inspection, of which 337 pertained to the public sector and 846 to the private sector. In comparison to the previous year, this represents an 11.5% increase in inspection procedures. On the basis of complaints against public sector legal entities it initiated 319 inspection procedures, while it initiated 18 procedures ex officio; furthermore, it initiated 770 inspection procedures on the basis of complaints against the private sector, while it initiated 19 procedures ex officio.

With regard to complaints, the largest number of suspected violations of the provisions of the GDPR/ZVOP-1 referred to the following:

- Unlawful disclosure of personal data; the transfer of personal data to unauthorised users by data controllers and unlawful publication of personal data (405 cases);
- Abuse of personal data for direct marketing purposes (150 cases);
- Unlawfully collecting or requiring personal data (114 cases);
- Unlawful video surveillance (112 cases);
- Inadequate security of personal data (96 cases);
- Unlawful access to personal data (83 cases);
- Processing personal data contrary to the purposes for which they were collected (36 cases);
- Hacker attacks and hacking into information systems (32 cases);
- Refusing to delete personal data (31 cases);
- Cookies (13 cases);
- Refusing to grant access to personal data (10 cases);
- Other (38 cases).

In 2019, the Information Commissioner received 137 data breach notifications. 80 notifications were sent by liable entities from the private sector (such as banks, telecommunications operators, insurance companies), and 57 by liable entities from the public sector (mainly health and education institutions).

Due to violations of the provisions of the ZVOP-1, 139 minor offence proceedings were initiated in 2019 (compared with 101 in 2018 and 105 in 2017), of which 83 were against legal entities from the public sector

and their responsible persons and 32 were against legal entities in the private sector and their responsible persons. 24 proceedings were against individuals.

In minor offence proceedings, including those initiated in previous years, the Information Commissioner issued 10 warnings and rendered 65 minor offence decisions (44 fines and 21 cautions). Furthermore, the Information Commissioner issued 54 additional warnings for minor violations, which is in line with the principle of procedural economy. In response, the suspected offenders filed a total of 10 requests for judicial protection.

The Information Commissioner emphasizes that conducting minor offence proceedings and imposing sanctions for established violations were greatly influenced by the fact that Slovenia has still not adopted systemic legislation for the application of GDPR (the so-called ZVOP-2). The Information Commissioner was thus unable to initiate minor offence proceedings and impose sanctions for violations of GDPR; it could only do so for violations of those provisions of the ZVOP-1 that are still in force or only for liable entities to which the ZVOP-1 applies in full.

In 2019, the Information Commissioner received a total of nine decisions from local courts on requests for judicial review pertaining to this and past years' decisions. In six cases the court rejected the request for judicial review as unfounded, in two cases it granted the request for judicial review by modifying the Information Commissioner's decision on the minor offence as it related to the decision on the sanction and issued a reprimand to the offender instead of a fine, and in one case the minor offence proceedings were terminated (the judgment is not yet final as the IC has lodged an appeal against it).

COOPERATION IN CROSS-BORDER INSPECTION PROCEDURES

In 2019, the Information Commissioner examined 148 cross-border cooperation procedures according to Articles 60 and 61 of the GDPR with regard to the controllers who perform cross-border personal data processing, whereby in 77 procedures it identified itself as the concerned supervisory authority (according to Article 56 of the GDPR).

The basis for performing cross-border cooperation according to Article 60 of the GDPR is the definition of a lead supervisory authority and supervisory authorities concerned according to Article 56 of the GDPR. In 77 such procedures in 2019, the Information Commissioner identified itself as the authority concerned. Seven investigative procedures were initiated by the Information Commissioner on the basis of a reported alleged breach of personal data protection in a cross-border case. 70% of the investigative procedures were initiated at the initiative of other authorities in the EU, and the Information Commissioner identified itself as the supervisory authority concerned.

On the basis of the procedures for determining the lead supervisory authority and the supervisory authorities concerned, in 2019 the Information Commissioner actively participated in 75 cross-border cooperation procedures related to the inspection of companies with cross-border operations. 14 of these cooperation procedures were initiated by the Information Commissioner on the basis of a report or complaint received against the actions of an entity established in another EU Member State or in various EU Member states or whose actions related to personal data processing affected individuals from various EU Member States. 61 of these procedures were initiated by other authorities in the EU and they were often in relation to popular online service providers, also known as internet giants (Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft, etc.). In 2019, eight draft decisions and one final decision according to Article 60 of GDPR were issued in cases in which the Information Commissioner cooperated.

In 2019, the Information Commissioner cooperated in 73 procedures for providing mutual assistance between supervisory authorities according to Article 61 of GDPR. In 40 cases, it responded to the requests by other authorities, and 33 requests for cooperation were sent to other authorities in the EU.

SELECTED CASES OF PROCESSING OF PERSONAL DATA

Ransomware

The Information Commissioner received multiple complaints regarding the breach of personal data protection that were the result of a ransomware attack. Attackers use ransomware, which is a type of malware, to lock and encode the data on the victim's computer or device and then demand ransom to re-enable access. Some ransomware (e.g. Cryptolocker) encodes user files with a key that only the attacker knows, while other ransomware (e.g. Winlocker) blocks access to a system, but leaves the files untouched. The GDPR provides guidelines regarding safeguards in the field of personal data protection to data controllers and processors, as it stipulates in Article 32 that in assessing the appropriate level of security, account of the risks that are presented by processing shall be taken, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. The decision on what security level a particular body must implement is therefore in the hands of the body itself, whereby account is taken of the state of the art and the implementation costs as well as the scope, context and purposes of the processing, the risks to the rights and freedoms of natural person of varying likelihood and severity.

Unlawful inspection of personal health data and obtaining the data of the employees performing such inspections

In 2019, several hospitals notified the Information Commissioner in accordance with Article 46 of the Patients' Rights Act that there had been unlawful inspections of patients' personal data, which were discovered within their internal procedures. The Information Commissioner also received some complaints from individuals who wished to obtain the list of people who inspected their personal data. In these cases, the Information Commissioner introduces an inspection procedure only if the individual, in their complaint, shows specific reasons to suspect that employees of a particular controller performed unlawful inspections of the personal data in a particular period or that their personal data was processed for unlawful reasons (e.g. that a particular person has at their disposal data that they were only able to obtain by performing an unlawful inspection of a personal database). The mere assumption that some employees who have access to personal data used and processed such data unlawfully is not sufficient for introducing an inspection procedure. The employees in a particular healthcare institution can only inspect a patient's personal data if they are participating in the process of their medical treatment or for other legal reasons (e.g. for the purpose of issuing an invoice for medical services or for the purpose of the compulsory reporting of particular cases to the police or other authorised users). If the suspicion of an unlawful inspection of patients' personal data is confirmed, the Information Commissioner issues a fine to the violating party due to the unlawful personal data processing. Based on the unsuitable protection of passwords, a fine is also issued if an employee attempts to avoid their responsibility by stating that their password was abused by a third person.

Notifying individuals on personal data processing

In addition to the lawfulness of personal data processing, personal data controllers must also ensure the fairness and transparency of its processing. This is done by providing individuals with appropriate information on personal data processing. Providing information to individuals according to Article 13 of the GDPR must be carried out regardless of what the legal basis for personal data collection is (consent, legal interests, performance of a contract, etc.). The manner of providing information depends on the manner of personal data collection and is only deemed to be suitable if the controller can later prove that they truly provided suitable information to individuals upon collection. The selection of the suitable manner of notification depends on the circumstances of a specific case, but it is important for the information to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, as stipulated by Article 12(1) of the GDPR. Suitable information must also be available to individuals when personal data is provided online, so a website must be designed so that an individual must read the prescribed information before entering or providing their personal data. With regard to this, the Information Commissioner advises that, when preparing information, the controller does this for the purpose of processing the personal data set forth by law or determined by the controller. The purposes of personal data processing must be defined as precisely as possible and must not be subject to the subsequent will of the personal data controller. In order to assist controllers in providing information, the Information Commissioner drafted the form 'Notification to Individuals according to Article 13 of the General Data Protection Regulation with Regard to Personal

Data Processing', which is available at https://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/.

Disclosing personal data in the decisions of social work centres

For a number of years, the Information Commissioner has been receiving numerous complaints against social work centres, in which the applicants state that they filed an application with a centre for the exemption from the payment of surcharges for institutional care costs, but then received a decision in which all of their income is listed, including the income of their partners, and the centre served the decision to some of their relatives as well. On the basis of these complaints, the Information Commissioner did not initiate an inspection procedure, as personal data processing in this case is carried out in the administrative procedure in which decision is reached on the payment of institutional care. In considering personal data processing in specific administrative procedures, the Information Commissioner is obliged to observe the Decision of the Constitutional Court No U-I-92/12-13 of 10 October 2013, in which the Court decided that there is no basis for the Information Commissioner to interfere with how procedures are managed, procedural actions are carried out, and decisions are made by authorities subject to public law in individual and specific matters, and that the Information Commissioner may not verify whether personal data protection is observed in these procedures and is carried out in accordance with the law and the Constitution. The individuals who received a decision from a social work centre therefore have the opportunity to enforce their rights within the scope of the legal remedies that are available to them in a specific administrative procedure and that are listed in the indication of legal remedies in the decision (i.e. appeal may be filed to the Ministry of Labour, Family, Social Affairs, and Equal Opportunities). Even though inspection procedures are not introduced due to lack of competence, the Information Commissioner explains to the applicants on which legal basis social work centres process personal data within the decision-making procedures for the exemption of payment for institutional care. Pursuant to paragraph three of Article 37 of the Exercise of Rights from Public Funds Act (ZUPJS), the right to enforce an exemption from payment for social protection services enforced by a entity who is liable to do so according to social care regulations is enforced by filing an independent application in addition to the eligible person's application for enforcing the exemption from the payment of social protection services. In this case, a social work centre issues a single decision to rule on the rights and obligations of the eligible person and the liable entity. In accordance with paragraph two of Article 37, the explanatory note of the decisions on the rights arising from public funds contains the type and amount of the income referred to in Article 12 of the said Act and the type and value of the assets referred to in Article 17 of the said Act, which were taken into account when calculating the income per family member. Therefore, a social work centre does not have the option not to state the income and assets of all persons liable to pay institutional care costs in the decision on the eligibility for the exemption from the payment of institutional care costs. The decision must be served to all persons liable for payment, who are thus informed of the personal data of the other persons liable.

Video surveillance from a private home

Every year the Information Commissioner receives quite a few complaints against individuals who have installed cameras on their homes, which they use for video surveillance of their own property and their neighbours' property and/or public property as well. According to Article 2(2)(c) of the GDPR, video surveillance carried out by an individual from their home is considered to be the processing of personal data by a natural person in the course of a purely personal or household activity, except when public areas not owned by them are also recorded. This position arises from the judgment of the EU Court of Justice in the case Ryneš proti Úřad pro ochranu osobních údajů, No C-212/13 of 11 December 2014. In order to initiate an inspection procedure against an individual carrying out video surveillance with cameras on their own property, on which no registered business activities are carried out, the Information Commissioner needs proof regarding the unlawfulness of the video surveillance, e.g. a specific video showing that the individual is using their video surveillance system to actually record areas not owned by them and that the quality of these videos is such that an individual can be recognised from the video. This is not proven just by having cameras on the exterior of a house, as it cannot be determined merely on the basis of an installed camera what this camera is actually recording, if anything at all; individuals can also install blind cameras that do not actually record anything, but have a preventive effect, or the quality of the recordings is so poor that the recorded persons cannot even be recognised.

If the applicant submits suitable evidence, the Information Commissioner can initiate an inspection procedure to assess whether there is a legal basis for an individual to carry out video surveillance of public

areas for the purpose of protecting their property in accordance with Article 6(1)(f) of GDPR, which stipulates that personal data processing (video recordings) is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. The legal interest of the person carrying out video surveillance is based on Article 33 of the Constitution of the Republic of Slovenia, which stipulates the right to private property, and Article 34, which stipulates the right to personal dignity and safety. Whether the performance of video surveillance and the recording of public areas by an individual are permitted mainly depends on whether they are able to effectively protect their property in another manner or not. If an individual proves that the recording of a part of a public area is lawful, they must post a notice of video surveillance. In cases when an individual does not record public areas, but the property of another individual, the Information Commissioner usually does not initiate an inspection procedure, as the affected individual may enforce their rights within criminal or civil proceedings.

The right to erasure of the personal data published in online media

After the GDPR entered into force, the Information Commissioner received some complaints by individuals because personal data controllers (media companies) rejected their requests to erase personal data or articles containing their personal data from their websites. When reaching a decision concerning the complaint of an individual, the Information Commissioner first verifies whether the published data is subject to protection according to the ZVOP-1 or the GDPR, i.e. whether it is a part of personal data filing systems or is processed by automated means. Furthermore, the Information Commissioner assesses whether the data listed in the article is adequate, relevant and limited to what is necessary for media reporting, whether any of the erasure conditions have been met, and whether there are grounds for an exception on the basis of which the erasure of personal data is rejected.

In particular, the provision of Article 17(3)(a) of the GDPR must be taken into consideration when assessing whether an individual's request for the erasure of data by a media company is founded; this provision excludes the right to erasure and stipulates that an individual does not have the right to erasure of their personal data if this data needs to be processed for exercising the right of freedom of expression and information. The freedom of expression is regulated by Article 39 of the Constitution of the Republic of Slovenia and Article 10 of the European Convention on Human Rights, whereby the decisions by the Constitutional Court of the Republic of Slovenia emphasise that the freedom of speech is particularly significant in cases of expression within journalism, as the broad boundaries of the freedom of press are one of the bases for a modern democratic society. It is evident from case law that the European Court of Human Rights developed a set of criteria for the balance between the right to privacy and the right to freedom of expression, which must be taken into account, including: the contribution to a discussion in the public interest, how well-known the person to whom the publication refers is, what the subject of the publication is, the prior conduct of the person to which the publication refers, the substance, form, and consequences of the publication, the method and circumstances of gathering information, and the veracity thereof. The allegations of the individual that they have incurred damage due to the publication of particular data or due to the free access to particular articles do not affect the assessment of the right to erasure. This right is only assessed according to the criteria set forth in Article 17 of GDPR. If an individual thinks that an article contains allegations or false information that could harm their honour and good name and cause them damage, they have the right to legal recourse, the competence for which lies with courts.

Enforcing rights with controllers from other EU Member States

The Information Commissioner receives complaints and reports by individuals from Slovenia regarding the enforcement of their rights according to the GDPR that might refer to controllers from other EU Member States, e.g. employers in case of neighbouring countries or online service providers with cross-border accessibility. The complaints may refer to the fact that a controller does not allow an individual to be informed of their own personal data, that they do not fulfil the right to data erasure, etc. In the case of cross-border personal data processing (the controller is based in another EU Member State), the Information Commissioner first locates the body that is competent for examining the matter according to their territorial competence or as the main authority in a cross-border cooperation procedure. If cross-border cooperation is not in question, but this is an individual case of breach in another EU Member State, the Information Commissioner uses cooperation mechanisms referred to in Article 61 of GDPR and submits the complaint to the competent supervisory authority for examination. When a report or complaint due to the failure to fulfil the rights of individuals is not only individual in nature but indicates a systematic failure by a controller carrying out cross-border data

processing, the first step in examining a case includes a procedure for determining the lead authority and authorities concerned according to Article 56 of the GDPR. The Information Commissioner sends an English translation of a report or complaint to the competent authority and actively cooperates with this authority by way of informal consultations until the final decision is issued. Cross-border cooperation procedures according to GDPR are a very welcome new tool in fulfilling rights, which have shown promising results. The cases that the Information Commissioner was unable to officially submit prior to GDPR due to restrictions regarding territorial competence can now be effectively resolved in favour of the rights of individuals.

Control over tech giants due to personalised advertising

The providers of popular online services, social networks, and communication platforms (Facebook, Google, Twitter, Amazon, etc.) very often monetise their free services with the help of personalised and targeted advertising based on the processing of massive quantities of data on individuals. The practices of using personal data are often unseen to ordinary users of services, but can, at the same time, have a very negative effect on their right to personal data and privacy protection. They may lead to discrimination and social stratification; the use of data of individuals for political promotion ahead of elections and referendums via social networks is particularly problematic. As the supervisory authority concerned, the Information Commissioner cooperates in a number of procedures against these companies and their personal data processing for the purpose of personalised advertising, also on the basis of reports and complaints by non-governmental and consumer organisations and their findings in recent reports[1]. In most cases, the lead supervisory authority is the Irish supervisory authority for personal data protection. The procedures are ongoing and at the level of consultations between supervisory authorities; the first decisions are expected to be reached in 2020. As the supervisory authority concerned in these procedures, the Information Commissioner may file a formal objection to the draft of the decision composed by the lead supervisory authority. The lead authority must take into account these objections by supervisory authorities concerned when composing the final decision according to Article 60 of GDPR. If the lead supervisory authority and the supervisory authorities concerned do not agree regarding the final decision or the objections of the supervisory authorities concerned are not taken into account, the matter is submitted to the European Data Protection Board, which adopts a decision according to Article 65 of the GDPR.

[1]E.g.: https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf, https://brave.com/wp-content/uploads/ 2018/09/Behavioural-advertising-and-personal-data.pdf

3.3 OTHER ADMINISTRATIVE PROCEDURES

Implementation of biometric measures

The Information Commissioner received 6 applications regarding the implementation of biometric measures. 2 applications have been withdrawn by the applicants, and 3 decisions on the permissibility of such measures were issued. One controller was permitted to implement biometric measures by using a fingerprint scanner, namely for the entry into secure rooms, where the most sensitive processes related to digital asset management are carried out. One application was refused because the applicant wanted to introduce biometric measures using a facial recognition and fingerprint recognition device to simplify the procedure of registering their employees' work time. Biometric measures that are only introduced for convenience or because they are more economical than other work time registration systems cannot be designated as necessarily required for fulfilling the purposes defined in paragraph one of Article 80 of the Personal Data Protection Act (ZVOP-1). One application was partially granted and the applicant was permitted to implement biometric measures using a fingerprint scanner as the only way of entering a server room where servers and other IT equipment and assets are located. However, the applicant was not permitted to implement biometric measures at the main entrance to the office building because this building is entered by a large number of individuals (all of the employees and visitors) using RFID cards.

Connecting filing systems

In 2019, the Information Commissioner received 24 applications for permission to connect filing systems. In 23 cases, the applicants were allowed to connect filing systems.

Transfer of personal data

According to GDPR, the permission of the Information Commissioner is generally no longer required for the transfer of data to third countries or international organisations, other than in limited cases of transfer on the basis of the safeguards referred to in Article 46.

In 2019, the Information Commissioner received one application for the authorisation of an administrative arrangement referring to the transfer of personal data obtained when performing tasks, powers and responsibilities between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities, such as public authorities, regulators, and/or financial market authorities responsible for the regulation and supervision of securities and/or derivatives markets. On 12 February 2019, the European Data Protection Board also issued a favourable opinion with regard to the Administrative Arrangement for the Transfer of Personal Data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities. The Information Commissioner found in the procedure that this specific administrative arrangement provides suitable safeguards and grants the individuals to whom the personal data refers enforceable rights and effective legal remedies. Therefore, it permitted the applicant to transfer the personal data obtained when performing tasks, powers and responsibilities to financial supervisory authorities in third countries with which they will sign the said administrative arrangement after receiving a decision on the basis of the administrative arrangement arising from Article 46(3)(b) of the GDPR.

Data subjects' rights

In 2019, the Information Commissioner received 181 appeals regarding the right of individuals to access to personal data, which is an 82% increase in comparison to the previous year. 70 appeals concerned public sector controllers and 111 controllers from the private sector. The Information Commissioner issued 38 administrative decisions (which is 50% more than in 2018). In 19 decisions, it ruled fully in favour of individuals and ordered the controllers to provide specific personal data, while in 11 decisions, it only partially ruled in favour of the applicants. In 8 decisions, it dismissed the complaints filed by individuals as unfounded. The Information Commissioner dismissed 33 complaints by an order.

3.4 OPINIONS AND CLARIFICATIONS

General clarifications

In 2019, the Information Commissioner issued 1,261 written opinions and referrals to previously published opinions. Around 5,000 opinions are already published on the website https://www.ip-rs.si/vop/, which are categorized into 48 substantive areas. Users can browse through opinions issued prior to the entry into force of the GDPR and, with the use of a separate search engine, browse through opinions issued after 25 May 2018. The Information Commissioner also encourages seeking advice and answers to questions over the telephone. Thus, a Data Protection Supervisor is on duty every day to answer such calls. In 2019, state supervisors received 2,023 calls.

Participation in the preparation of laws and other regulations

The Information Commissioner issues opinions on regulations in accordance with the provisions of Article 57(c) of the GDPR and Article 48 of the ZVOP-1. In 2019, the Information Commissioner issued 75 opinions on proposed amendments to legislation and proposed new laws and regulations. Despite a slight increase in the number of such opinions, it is still much lower than before 2018, when the Information Commissioner issued more than 100 opinions per year.3

3.5 COMPLIANCE AND PREVENTION

In 2019, the Information Commissioner strengthened the area of its competence that deals with **compliance, prevention and information technology**. Employees with legal, technological and communication skills work in this area to prepare materials and communicate with the liable entities.

Contractual processing

In 2019, the Information Commissioner detected a general trend of a significant increase in entering into agreements on contractual personal data processing between liable entities. The number of opinions related to contractual processing posted by the Information Commissioner on its website has nearly tripled since 2018 (the number of opinions from the 'contractual processing' section by year: 2016: 8, 2017: 11, 2018: 17, **2019: 47**).

In 2019, the Information Commissioner also began drafting standard contractual provisions, which will be of great help to liable entities in arranging their contractual relationships. Pursuant to a prescribed procedure, standard contractual provisions will be confirmed by the European Data Protection Board in 2020.

Records of processing activities

Within a privacy sweep, the Information Commissioner asked 130 of the largest employers in the country to record personal data processing activities for data that is collected when using employees' work assets, such as the internet, e-mail, printers, etc. These included 40 employers from the public sector and 90 from the private sector; together they employ approximately 146,000 people. 67 liable entities, employing approximately 84,000 people, responded to this request (the response was not mandatory). For prevention purposes, the Information Commissioner also asked 40 online retailers to comply; 21 of them responded.

Personal data impact assessments

In 2019, the Information Commissioner issued opinions regarding the following impact assessments within a prior consultation procedure: Opinion on the assessment of impacts on personal data protection relating to the use of the 'Certificate regarding justified sick leave in electronic form' (eBOL) system; opinion on the assessment of impacts on personal data protection regarding the proposed amendment of the Central Credit Register Act (ZCKR); opinion on the assessment of impacts on personal data protection when introducing a system for renting electrical vehicles, etc.

The Information Commissioner finds that the knowledge and quality of the drafted impact assessments are improving, but liable persons are still paying insufficient attention to risks related to enforcing the rights of individuals.

Data protection officers

By the end of 2019, **2,150 liable entities reported the designation of a data protection officer**, and the Commissioner's staff frequently spoke at public events on data protection officers' duties, their position and designation. The Information Commissioner also designated its own data protection officer and established a dedicated electronic mailbox dpo@ip-rs.si.

In some way, data protection officers are the extension of the Information Commissioner, so the Information Commissioner will pay more attention to them in 2020, mainly by promoting and enabling their interconnection, the exchange of experience and practice by taking into account specific features in the field.

Codes of conduct and certification

In 2019, the Information Commissioner received only one draft code of conduct, which was submitted by an ineligible data subject and was thus not considered. The Information Commissioner notes that associations, chambers, federations and similar bodies could invest more energy in drafting such codes, thus relieving their members of some burden and providing uniform legal practice, procedures and operation which is, above all, validated by the supervisory authority.

The GDPR also provides for the possibility of certification, although this still requires the development of appropriate accreditation and certification systems; activities are still ongoing at the EU level.

Training and awareness raising activities

The Information Commissioner was once again very active in training and awareness raising activities in 2019, particularly through the Information Commissioner's website (www.ip-rs.si) and through various materials; it organised various events and free lectures, it was present on social media, and it also worked with some other organisations and on various projects.

The Information Commissioner also prepared different materials, namely:
- Guidelines: Guidelines on Personal Data Protection in Employment Relationships; Guidelines on the Tools for Privacy Protection on the Internet; Guidelines on the Use of GPS Tracking Devices and Personal Data Protection
- Recommendations: Recommendations on Arranging Joint Personal Data Management;
- Forms: A form for enforcing the personal data portability right (Article 20 of the GDPR); Application for the transfer of personal data to third countries or international organisations.

Infographics that present certain thematic areas, which are very complex, in a simple and effective way: Reporting a data protection breach: unjustified inspections of personal data; infographics on contractual processing; transfer of personal data according to the General Regulation to third countries and international organisations in two steps, etc.

The Information Commissioner also **organized and conducted numerous events**. On the occasion of European Data Protection Day, it organized a special event on the GDPR and presented awards for good practices in the public and private sectors, a special Privacy Ambassador Award and awards to the recipients of the information security management certificate ISO/EIC 27001: 2013. The 2019 Privacy Ambassador Award went to the Slovenian Consumers' Association. In 2019, the Information Commissioner delivered 102 pro bono lectures on the novelties of the GDPR to various chambers and associations in the public and private sectors and at conferences and seminars.

The Information Commissioner also participates in various projects. In 2019, it continued activities within the framework of the European project **RAPiD.Si** (Raising Awareness on Data Protection and the GDPR in Slovenia) aimed at educating and raising awareness of small and medium-sized enterprises and individuals on the reform of the legislative framework in the field of personal data protection. The Commissioner cooperated with the Slovenian Consumers' Association and prepared regular articles for ZPSTest magazine. It also issued a Guide on consumers' personal data protection, titled 'You decide'.

3.6. INTERNATIONAL COOPERATION

As the national supervisory authority for the protection of personal data, the Information Commissioner cooperates with the competent bodies of the European Union (EU) and the Council of Europe engaged in personal data protection. The Information Commissioner also actively participated as a member of the European Data Protection Board (EDPB), which is an independent European body for ensuring the consistent application of data protection rules in the EU and for promoting cooperation between EU data protection bodies; it has been operating since May 2018. Representatives from all 28 independent supervisory authorities in the EU and the EEC (Iceland, Norway and Liechtenstein), the European Commission, and the European Data Protection Supervisor participate on the Board. The Board operates in accordance with its rules and guiding principles.

In addition, the Commissioner participated in six working bodies of the EU, which oversee the implementation of personal data protection in the context of large EU information systems.

In 2019, amendments to the procedural rules of the EDPB were also adopted, on the basis of which a new supervisory authority was established – the Coordinated Supervision Committee (CSC – a committee for the coordinated supervision of personal data processing within large EU information systems). Over time, the supervision of large EU information systems will move under the umbrella of the CSC.

In May 2019, an evaluation of the implementation of the Schengen acquis from the perspective of personal

data protection was successfully carried out; the Information Commissioner also actively participated in this evaluation.

In 2019, the Information Commissioner continued to participate in the Council of Europe's Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

The Information Commissioner also actively participated in the International Working Group on Data Protection in Telecommunications (IWGDPT), bringing together representatives of information commissioners and data protection and privacy authorities from all over the world.

INITIATIVE 20i7
In 2017, the Information Commissioner launched "**Initiative 20i7**" in order for data protection supervisory authorities from the former Yugoslavia to join forces, as they face similar professional issues and challenges. The objective of Initiative 20i7 is to foster close cooperation and exchange good practices in the area of personal data protection in the region. At the third Initiative 20i7 meeting, which took place in May 2019 in Budva, the representatives of the supervisory authorities for personal data protection from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo, North Macedonia and Slovenia exchanged their experience and practices in implementing and approximating to the standards introduced by the General Regulation.

3.7 GENERAL ASSESSMENT OF THE SITUATION REGARDING PERSONAL DATA PROTECTION

In 2019, the work of the Information Commissioner in the field of personal data protection was mostly characterised by the GDPR, the direct application of which began in all EU Member States on 25 May 2018 and which additionally expanded the tasks and powers of the Information Commissioner according to the ZVOP-1. Due to the need to adjust the field of personal data protection, the scope of activities performed by personal data controllers and the Information Commissioner significantly increased. The GDPR and the Directive for criminal prosecution authorities require that a new systemic Personal Data Protection Act (ZVOP-2) be adopted, by way of which their implementation would be fully ensured in the Republic of Slovenia. As of 2019, the Republic of Slovenia has not yet adopted such an act. As a result, there are many open questions, a lack of clarity and mainly practical issues for personal data controllers, processors and the Information Commissioner.

The failure to adopt the new ZVOP-2 has not significantly affected the implementation of inspection, but it has affected the conduct of complaint procedures initiated by individuals regarding the enforcement of their rights referred to in Articles 13 to 22 of the GDPR, in which the Information Commissioner acts as the complaint authority. The scope of the rights of the data subject and the related competences of the Information Commissioner as the complaint authority have significantly increased compared to the current ZVOP-1; for this reason, the number of such complaints also significantly increased in 2019 compared to the previous year. In order for these complaints to be resolved, special rules need to be determined, by way of which individual administrative procedure issues could be resolved and used to set forth the procedure for the resolution of complaints. Therefore, the failure to adopt the new Personal Data Protection Act (ZVOP-2) resulted in quite a few dilemmas that arose when managing such complaint procedures.

The failure to adopt the ZVOP-2 had a particularly negative effect on managing minor offence proceedings and giving fines for discovered breaches, because the Information Commissioner was only able to, in the absence of the ZVOP-2, order entities subject to inspection to eliminate the irregularities discovered, establish legal conditions and ban any unlawful personal data processing; minor offence proceedings could only be initiated in the event of a violation of those ZVOP-1 articles that are still in effect or in the event of a violation committed by entities subject to the Directive for criminal prosecution authorities. Therefore, due to the absence of the ZVOP-2, the Information Commissioner was unable to impose sanctions for those breaches that are only set forth in Article 83 of the GDPR, but was able to, within minor offence proceedings, sanction the breach of those articles of the still valid ZVOP-1 that are not in conflict with the GDPR. For this reason, the Information Commissioner has warned the competent ministry multiple times of the necessity of adopting the new Act and of harmonising and coordinating the minor offence provisions in the ZVOP-2 with the provisions of the GDPR. The harmonisation of the national provisions with the GDPR is

particularly important from the perspective of coordinating the practices in the EU Member States in which the GDPR is applied. The EDPB, of which the Information Commissioner is a member, is working on forming a mechanism for coordinating imposed fines, which should be used by all supervisory authorities and which is based on the criteria for imposing fines in a manner and in the amount set forth by Article 82 of the GDPR. The purpose of the mechanism is coordination: the fines imposed for similar minor offences in similar circumstances should not differ from country to country, which is particularly true in cases of cross-border cooperation regarding inspections.

The number of complaints that the Information Commissioner received in 2019 increased compared to previous years: The Information Commissioner received 974 complaints or requests to initiate an inspection procedure, which is the highest number thus far.

In addition to the aforementioned complaints, in 2019, the Information Commissioner received and examined another nine cases of unlawful notification or other unlawful personal data processing regarding patients, which were sent by healthcare providers pursuant to Article 46 of the Patients' Rights Act (ZPacP), and 137 official data breach notifications sent by personal data controllers. The submission of such official notifications regarding personal data protection breaches, i.e. voluntary disclosure, is a new mechanism imposed on personal data controllers and processors by Article 33 of the GDPR. According to current findings, companies and controllers use such official notifications regarding personal data protection breaches to quite diligently report security incidents to the Information Commissioner.

Personal data controllers most frequently sent official notices regarding personal data protection breaches to the Information Commissioner due to the loss or theft of personal data storage media (e.g. personal computers and USB sticks), unauthorised access to personal data due to software errors or the abuse of power committed by employees, a hacker attack on the IT system, preventing access to data due to encryption using malicious code, and forwarding personal data to unauthorised or wrong persons.

When examining complaints received by individuals, the Information Commissioner finds that the complaints are often filed due to a lack of understanding of the provisions of the GDPR, which is particularly true when processing personal data on the basis of the consent provided by the data subject. Although it is true that the GDPR sets forth stricter conditions to be fulfilled in order for a consent to be considered valid, the consent of the data subject is only one of six equal legal bases that are stipulated by Article 6 of the GDPR regarding the lawfulness of personal data processing. For this reason, it often turned out when examining complaints that controllers obtained consents from data subjects even when the personal data processing was set forth by law or was necessary for fulfilling an agreement with the data subject, or another condition referred to in Article 6 of the GDPR was fulfilled, which meant that the consent of the data subject was not even necessary.

Complaints and breaches of the GDPR also often occurred because controllers failed to provide individuals relevant or complete information when collecting personal data. Controllers are obliged to adopt suitable measures by way of which they, when collecting personal data, provide the data subject with the required information regarding personal data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The types of information that need to be provided to the data subject when their personal data is collected are set forth in Articles 13 and 14 of the GDPR, while the data subject discovers on the basis of such information who the personal data controller is, for what purposes and on which legal basis the personal data is processed, who the recipients of the personal data are, how long the data is stored, etc. Breaches of the provisions of Articles 13 and 14 of the GDPR were still among the most frequently discovered in 2019, despite the awareness-raising performed by controllers and samples of such notifications being drafted by the Information Commissioner and posted on its website. If a breach of the provisions of Articles 13 and 14 of the GDPR is discovered, the Information Commissioner orders that the discovered irregularities be eliminated, and after ZVOP-2 enters into force, the Information Commissioner will also be able to impose the fines set forth in Article 83(4) of the GDPR.

When examining complaints and performing preventive inspections, which the Information Commissioner carried out in 2019 with liable entities in the fields in which, considering the risk assessment, there is either a greater likelihood of a breach of personal data protection regulations or there is a greater risk of major harmful effects for data subjects in the event of breaches due to the sensitivity of personal data processing, it has been found that the discovered irregularities or deficiencies are still largely the result of

a lack of knowledge or understanding of legislation, which is also due to the fact that the ZVOP-2, which would more clearly determine individual rules regarding the implementation of the GDPR, has still not been adopted. In addition to the lack of knowledge regarding regulations, the discovered breaches are often the result of negligent or improper provision of personal data protection and intentional unlawful personal data processing by the employees working for personal data controllers, mainly in the form of unlawful inspections of personal data filing systems, disputable personal data processing for the purposes of direct marketing, and performing video surveillance of work premises with the purpose of controlling employees.

Similarly to previous years, the Information Commissioner conducted multiple inspection procedures and minor offence procedures due to unlawful inspections of personal data filing systems by employees, who performed such inspections either due to curiosity or in order to obtain personal data for their own purposes. Employees most frequently unlawfully inspected personal data filing systems in the field of internal affairs or the police as well as the personal data filing systems kept by healthcare institutions. The said personal data filing systems provide traceability of personal data processing, which means that it can later be discovered who inspected the personal data of an individual at a particular time; the employees whose work enables them to have access to the personal data in a filing system are informed of this, but unlawful inspections are performed nonetheless in the hopes of not being discovered. In the event of discovered breaches, the Information Commissioner issued a decision on a minor offence to all those who committed a breach, imposing a suitable sanction.

In 2019, the Information Commissioner continued its enhanced cooperation in the field of compliance and prevention. The Information Commissioner estimates that familiarity with the provisions of the GDPR improved in 2019 and that entities liable to observe the GDPR have a better understanding of its key concepts; however, numerous cases of legal confusion remain for controllers, which is the result of Slovenia failing to adopt a national regulation on the implementation of the GDPR and failing to transpose the Directive for criminal prosecution authorities into Slovenian legislation. According to the Information Commissioner, the appointment of personal data protection officers, of which there are more than 2000, also contributed to improvements, as their tasks include raising awareness, consulting and educating. The personal data protection officers are a kind of extension of the Information Commissioner, so, in the future, more activities will have to be devoted to them, as awareness-raising effects can multiply the more qualified these officers are, resulting in the compliance of entities liable to observe the GDPR. With regard to the remaining mechanisms of the GDPR arising from the principle of accountability, the knowledge regarding the assessments of impacts on personal data protection, which are an essential element in the preventive personal data protection, is improving, but there is insufficient awareness regarding the significance of the impact assessments as a key element in the procedure for preparing new regulations, which foresee serious interferences with the privacy of individuals and/or the introduction of modern technologies. The expectations concerning the codes of conduct to assist controller associations in reaching compliance were not met. Major associations apparently already have suitable resources and knowledge and seem to not see the added value of codes of conduct, while, according to our assessment, smaller associations do not have sufficient resources and knowledge to compose such codes. At the same time, the requirements of the GDPR regarding the bodies for monitoring the codes of conduct, which are mandatory for codes of conduct in the private sector, are very high, as they require financial, professional and human resource independence, which begs the question whether they are feasible. Due to the absence of national implementing regulations, the field of establishing data protection certification mechanisms and data protection seals and marks, to show that the processing actions performed by controllers and processors are in accordance with the GDPR, is also completely neglected.

According to the Information Commissioner's assessment, preventive activities for compliance, the implementation of which began in 2019, are a very effective method for achieving compliance. Most bodies liable for disclosing public information do not wish to violate the legislation and want to act in compliance with the law, so they need to be assisted in this and offered suitable tools, such as opinions, guidance, forms, infographics, etc. A very good example is the fulfilment of the duty regarding impact assessments performed for drone operators. On the basis of data from the Civil Aviation Agency, the Information Commissioner found that 77 liable entities failed to fulfil their duty regarding the performance of an impact assessment; after the Information Commissioner requested that they comply by sending suitable clarifications and instructions, only five such entities remained. Ensuring compliance by introducing inspection procedures against these many liable entities would certainly take a lot more time and require a lot more human and financial resources. Such activities proved to be especially effective in connection with associations of

liable entities who can distribute awareness-raising materials to their members and who also welcome this type of cooperation with the supervisory authority.

The Information Commissioner has successfully participated in the European Commission's calls for applications for projects from the REC programme (Rights, Equality and Citizenship Programme). In 2019, the RAPiD.Si project successfully continued, the main objective of which was to educate and raise the awareness mainly of small and medium-sized companies and individuals regarding the reform of the legislative framework in personal data protection, and, in 2020, the new iDECIDE project will begin, which is intended to raise awareness of the reform of the personal data protection framework, mainly among minors, the elderly and the working population.

The GDPR introduces important new developments with regard to the cooperation of personal data protection supervisory authorities in other EU Member States and EEC countries (Iceland, Norway and Liechtenstein) in cross-border cases according to the 'one-stop shop' principle, which foresees that the supervision procedure in a cross-border personal data processing case is conducted by what is known as the lead authority, which cooperates with other personal data protection authorities. Mutual assistance and joint operations mechanisms for personal data protection authorities in EU Member States was also introduced. In 2019, the Information Commissioner cooperated in 74 mutual assistance procedures with other supervisory authorities according to Article 61 of the GDPR and in 77 procedures for determining the lead authority according to Article 56 of the GDPR. Of these, seven procedures for such determination were initiated by the Information Commissioner. On the basis of the procedures for determining the lead supervisory authority and the supervisory authorities concerned, in 2019 the Information Commissioner actively participated in 75 cross-border cooperation procedures related to the inspection of companies with cross-border operations. In these procedures, it is expected that the decision of the supervisory authorities will be reached according to Article 60 of the GDPR, i.e. according to the 'one-stop shop' mechanism. 61 of these procedures were initiated by other authorities in the EU and they were usually in relation to popular online communication service providers, also known as internet giants (Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft, etc.); the Information Commissioner participates in these procedures as the authority concerned. The procedures examine the compliance of their practices with the GDPR, both in terms of the lawfulness of personal data processing as well as the adequacy of their privacy policies and policies on notifying data subjects regarding personal data processing, fulfilling the rights of individuals, and breaches of personal data protection due to IT system intrusions and insufficient personal data security. 14 of these cooperation procedures were initiated by the Information Commissioner on the basis of a report or complaint received against the actions of an entity established in another EU Member State or in various EU Member states or whose actions related to personal data processing affected individuals from various EU Member States.

Cooperation in cross-border inspection cases, as introduced by the GDPR, is undoubtedly one of the new key developments and enhancements, mainly in the sense of the unified operation of supervisory authorities in various EU Member States and EEC countries. Only by way of a unified approach can the supervisory authorities at the EU level affect the activities of multinational modern web service providers, communication platforms and social media used by individuals in all EU Member States and EEC countries, and the personal data protection supervisory authorities now also have at their disposal mechanisms and close cooperation tools, by way of which they have the opportunity of acting against disputable practices that harm the rights of data subjects with a single voice.

Of course, such cooperation poses a great challenge to the Information Commissioner, as well as other supervisory authorities: additional resources are required, both financial as well as human resources – the knowledge necessary for examining such cases is specific and it mainly includes very different disciplines. It is key to speak English very well, as English is the operational language in cross-border procedures. Conducting cross-border cases is complex and requires a lot of additional resources, including for the purpose of translating documentation (which can also encompass very comprehensive reports). Additional resources are required even just for administering cooperation using the IMI platform, which the Information Commissioner had to, in terms of organisation, integrate into its processes for examining inspection cases and cases related to decision-making concerning the right to be informed of one's own personal data. The Information Commissioner had to establish an internal system for tracking procedures in the IMI system and for connecting information with records kept at the national level. Therefore, the Information Commissioner had to allocate additional resources (equal to 4–5 regular employees) for the implementation

of Chapter VII of GDPR to ensure the internal coordination of cooperation processes and national practice regarding supervision and complaints, to provide education on the technical operation of the IMI system and on conducting cross-border procedures, unifying practices, and constantly tracking the practices being developed with regard to the use of the IMI system.

The experience from 2019 also showed that there were some other challenges for cooperation according to Chapter VII of the GDPR, particularly from the perspective of the differences between national procedural rules in EU Member States (e.g. regarding the rights of parties in procedures, concerning the deadlines for individual procedural actions, regarding sending notifications to applicants, etc.). Diverse national rules are certainly one of the reasons why the cooperation procedures according to the 'one-stop shop' principle are longer in more complex cases of supervision over large multinational companies. The first decisions in this context are expected to be reached in 2020. Different interpretations of the concepts and norms of the cooperation introduced by the GDPR, proved to be a major challenge to effectively conducting such procedures in specific cases in 2019. Answers are being sought by the EDPB, which is actively seeking common definitions and interpretations of the concepts from the GDPR, while, on the other hand, European legislation can also help resolve this issue, particularly by considering a potential future revision of the GDPR. The Information Commissioner submitted its positions regarding the application of Chapter VII of the GDPR for the purpose of carrying out audit procedures to the competent ministry, and it also contributed to the EDPB's positions regarding this topic.