15 YEARS

OF THE ACCESS TO PUBLIC INFORMATION ACT

1ST YEAR

OF THE GENERAL DATA PROTECTION REGULATION

ANNUAL REPORT

of Information Commissioner for 2018

'18

Introduction by the Information Commissioner

The year of 2018 was a breaking point in a certain way for both areas of Information Commissioner's work, with regard to the challenges and scope of work, as well as the content. In the area of access to public information we marked the 15th anniversary of the Access to Public Information Act (ZDIJZ). The area of personal data protection was, undoubtedly, marked by the General Data Protection Regulation (GDPR) coming into force, bringing numerous novelties in ways personal data are protected in the EU and, consequently also nationally. At the same time, the modernised Convention on personal data protection of the Council of Europe was adopted, disseminating the trend of changes far across the EU borders.

In the field of access to public information, the Information Commissioner handled 549 complaints in 2018 and once again recognised some positive indicators: on the one hand, the applicants are increasingly aware of their right to access to public information and, on the other, bodies liable respond more frequently to the applicants' requests. The upward trend in the number of complaints received over the last few years continued in 2018, which means that the applicants are well acquainted with their right to the legal remedy and are keen to use it. The complaints procedure is entirely free of charge and relatively swift for the applicants. Thus, the Information Commissioner considers that the complaints procedure provides an effective legal protection of the right to access to public information. In 2018, the Information Commissioner additionally reduced the average time of resolving the complaints, which has now settled at 32 days. The Information Commissioner considers the cooperation with the liable bodies in 2018 exemplary (in this year it did not initiate any minor offence proceedings in accordance with ZDIJZ, ZInfP or ZMed), but it still notes two trends: the number of complaints against the so-called administrative silence again rose this year and the number of complaints against municipalities increased after the trend was already downward before 2017.

The Information Commissioner received numerous requests for opinions and positions in 2018 as well, and it provided these in the context of its informal counselling on the basis of its established practice. This shows that throughout this year the bodies liable have been active and responsive and often asked turned to the Information Commissioner even outside complaints procedures, i.e. even when not prompted by a legal requirement. A relatively low number of administrative disputes brought against the Information Commissioner's decisions point to the fact that the bodies liable are willing to cooperate with the Information Commissioner and follow its recommendations. Thus, the bodies and the applicants respect and accept the Commissioner's decisions.

In the area of data protection, the Information Commissioner devoted the year of 2018 to the efficient start of the use of GDPR by raising awareness about the new regime among the data controllers and individuals. It also contributed comments in the process of development of the new law on data protection, and worked towards reorganization and strengthening of its organization, with a view of ensuring efficient enforcement and exercise of data subjects' rights, as well as other competencies of the Information Commissioner under the new regime and considering a notable increase of new cases. Similar to previous years, the Information Commissioner in 2018 received a large number of complaints from individuals. It handled 1029 inspection supervision cases (57% increase compared to the year before). The notable increase is undoubtedly a result of greater awareness of the individuals, since GDPR received a lot of media coverage. In May 2018 the Information Commissioner became the member of a new EU body – The European Data Protection Board, whose opinions are binding also for Slovenian DPA.

The experience after the first year of GDPR shows that its direct application constitutes a great challenge that will need a great deal of attention also in the following years. Especially because the Directive applicable to law enforcement agencies has not yet been implemented in the Slovenian legal regime, and the implementing laws regarding GDPR have not yet been put in place. In practice this brings many legal uncertainties for the private companies and other organizations, execution of data subject's rights and supervisory authorities. The information Commissioner, for example, does not yet have the authority to issue administrative sanctions in GDPR.

The Information Commissioner will, also in the future, strive to defend the achieved levels of transparency of the public sector and at the same time face the challenges, brought to the area of data protection by the new legislation and modern technologies. The work in both areas will be guided by pursuit of efficient protection and execution of individual's rights, in collaboration with the private and public sector entities and experts.

Mojca Prelesnik,
The Information Commissioner

THE INFORMATION COMMISSIONER

1.1 THE ESTABLISHMENT AND ID CARD OF THE INFORMATION COMMISSIONER

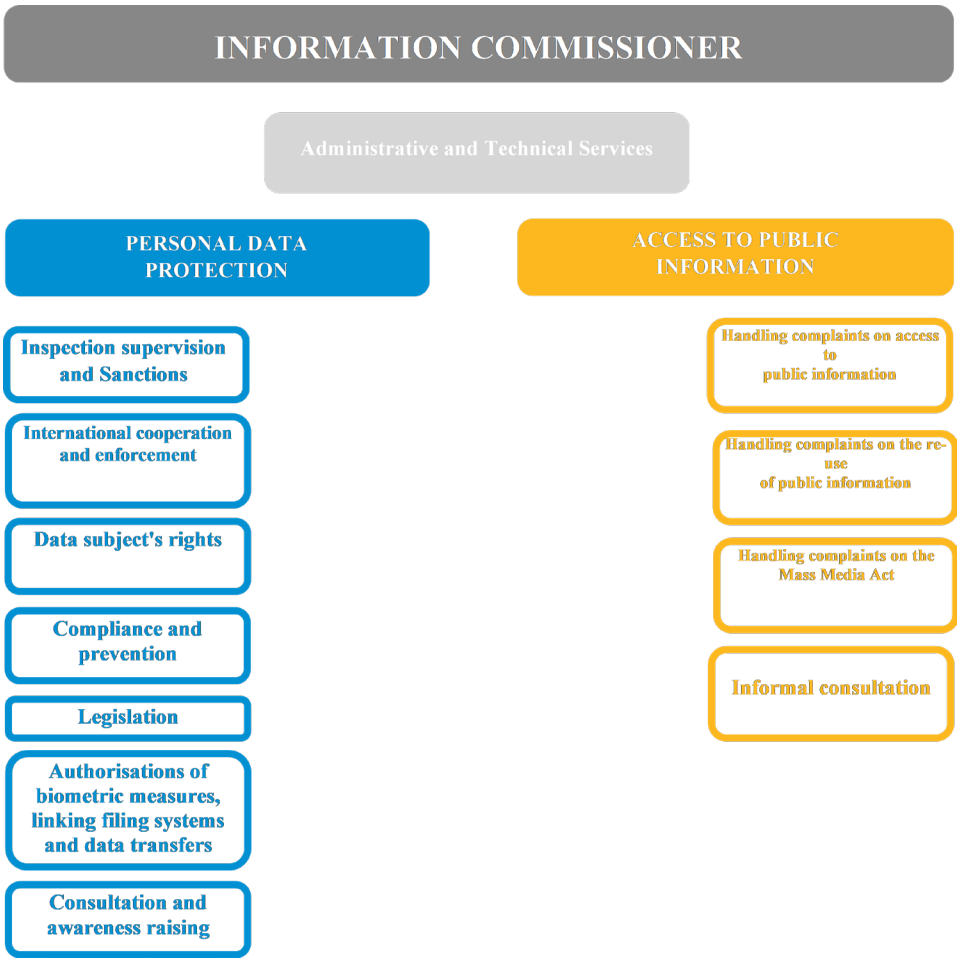
COMMISSIONER

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 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, the 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 responsibilities of the body responsible for the implementation of the right to access to 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.

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 2018, the Information Commissioner had 43 employees, of which three were employed on the basis of temporary contracts.

1.2 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 the 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, to 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 to perform other duties determined by these regulations;
- decide on the appeal of an individual against the refusal of a data controller to grant the request of the individual with regard to his right to access 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.

Entry into force of the General Data Protection Regulation hugely impacted the work of the Information Commissioner in the field of personal data protection in 2018. The GDPR is directly applicable in all EU Member States as of 25 May 2018. The Regulation requires the adoption of the 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 2018. Therefore, in addition to the GDPR, ZVOP-1 is still applicable, namely the provisions of the act which are not regulated by the Regulation and which do not contradict it.

In the area of access to public information, the Information Commissioner also has the 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.

1.3 FINANCIAL MANAGEMENT IN 2018

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 2018, the operating budget of the Information Commissioner amounted to EUR 1,833,399.66, of which EUR 1,490,391.00 were spent on wages and salaries, EUR 238,008.66 on material costs and expenses and EUR 104,551.45 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.)

On 1 August 2018, the Information Commissioner moved to new, leased premises at Dunajska cesta 22, Ljubljana. The spending was thus higher due to the cost of rent, operational costs, moving costs and refurbishing costs.

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

2.1 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

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

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 2018, the Information Commissioner received 549 appeals, of which 313 were against decisions refusing requests (19 of those appeals were against liable business entities subject to dominant influence of entities of public law), while 236 were against the non-responsiveness of first-instance authorities.

In appeal procedures the Information Commissioner issued 288 decisions on the merits, in five cases it rejected the appeal, while 7 applicants withdrew their appeals. In processing the appeals of individuals, 36 so-called in camera examinations were carried out.

The Information Commissioner received 236 appeals against the non-responsiveness of the authorities. The Information Commissioner first called on to the liable authorities to decide on the requests as soon as possible, which in most cases they did. In 21 cases the Information Commissioner rejected the appeal (in 19 of those cases because the appeal was lodged too soon and in 2 cases because the application was incomplete), in 22 cases it issued the explanation that it was not competent to consider their applications and advised the individuals how to act. 7 applicants withdrew their appeals as they received the requested documents and in one case the Information Commissioner transferred the matter to a competent authority for consideration.

In 2018, the Information Commissioner received 287 written requests for assistance and various questions of individuals regarding access to public information. During business hours the Commissioner also answered 640 telephone calls about questions from the field of access public information. The Information Commissioner replied to all applications to the extent it is competent, in most instances it referred them to the competent institution – The Ministry of Public Administration.

In 2018, 34 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 11,8 % 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.

The Administrative Court issued in 2018 40 judgments in relation to appeals filed against the decisions of the Information Commissioner. In 22 cases the Court dismissed the appeal, in 7 cases the Court granted the appeal and returned the matter to the Information Commissioner for reconsideration, in 6 cases it issued a decision rejecting the appeal, in 2 case the Court decided partially in favour of the appellants, in 2 cases it issued a decision staying the procedure and in 1 case it partially granted the appeal and returned the matter in relevant part to the first instance body for reconsideration.

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

- in 124 cases it dismissed the appeal;
- in 117 cases it partially or fully granted the appeal of the applicant or decided in favour of the applicant;

- in 40 cases it granted the appeal and returned the matter to the first instance body for reconsideration;
- in 4 cases it declared the first instance decision null;
- in 3 cases it rejected the appeal.

The following categories of bodies liable were the subjects of Information Commissioner's decision in the appeal process as they refused access to public information:
- public administration (ministries, constituent bodies, public administration units) (131 cases);
- public funds, institutes, agencies, public service contractors, and holders of public authority (86 cases);
- municipalities (50);
- liable business entities subject to dominant influence of the state, municipalities and other public law entities (21).

In 172 cases applications were submitted by natural persons, in 81 cases complaints were submitted by private sector legal entities. 29 complaints were submitted by journalists and 6 by public sector legal entities.

2.2 AWARENESS RAISING ACTIVITIES

The Information Commissioner performs a variety of activities for raising awareness of the specialised and general public. Among other activities, it organizes a yearly event to celebrate the Right to Know Day, which in 2018 was marked by the 15th anniversary of the Access to Public Information Act. Under the auspices of the President of the Republic of Slovenia, Mr. Borut Pahor, the Information Commissioner organized a panel discussion entitled "From Theory to Practice in Searching for Public Information: 15 Years of the Access to Public Information Act". On this occasion, the Commissioner also published the Information Commissioner's Practice Guide, a collection of numerous high-profile and interesting cases. The Guide aims at the liable bodies to help them face challenges specific to the field of access to public information.

The Information Commissioner's Practice Guide provides a concise overview of the most important cases and is freely available on the Information Commissioner's website.

On the occasion of International Right to Know Day, the Information Commissioner annually awards the Ambassador of Transparency Award. In 2018, the award was received by a team of journalists working for the broadcast "Tarča" of the RTV Slovenia, which for many years contributed to a better flow of information and transparency. In the framework of international cooperation, the Information Commissioner delivers lectures, papers and participates in workshops, thereby maintaining contacts with foreign countries and other supervisory authorities for access to public information.

2.3 SELECTED CASES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

Obtaining of impartial and objective information serves the public interest
The applicant (Transparency International Slovenia) requested access to a letter regarding the removal of transactions from the application "Erar" (an application dedicated to transparency of public money spending) relating to the procurement of protective technical barriers to secure the national border. The body liable granted access to the letter, but refused access to the list of transaction, as it was marked "internal" under the Classified Information Act (ZTP). The Information Commissioner found that the list was classified after the data was created, meaning that the formal condition for classifying the data was not properly fulfilled. Indeed, an assessment of the adverse consequences was created only after the optional information from list of transactions had been withdrawn from the publication in the Erar application. In addition, the material criterion for classifying the data was not fulfilled either, since neither the body nor the Institute for Commodity Reserves demonstrated that the disclosure of the requested document would cause or clearly could cause harmful effects for the security of the state or for its political and economic benefits. Above all, the Information Commissioner found there is an overriding public interest in the disclosure of the requested information. The media reported extensively on the fact that Slovenia used protective technical barriers at the border for regulating the migratory flows, on what type of barriers were used and what kind of problems emerged in this regard. Official information regarding all this also exists (e.g. in a reply to a parliamentary question). The Information Commissioner thus found that it is in the public interest to fully disclose the list of transactions in order to properly and comprehensively inform the public of the use of public funds in connection with the procurement and installation of technical barriers.

KEYWORDS: classified information, public interest test, decision number 090-298/2017

The amount of payment together with names and surnames of mentors engaged in relation to completing the study programs are publicly available

The applicant (journalist) requested information on how many payments did the Faculty of Law in Maribor or The University of Maribor make to individual professors and other associates in relation from the item "Scientific Master's Degree Programme". The liable body denied access to the applicant, as the requested information was allegedly obtained or drawn up for the purpose of the supervisory process (exception from Article 5a of the ZDIJZ). A performance audit of members of the University of Maribor was underway, examining among others the payments made to the professors. The Information Commissioner found that the exception to free access does not apply, because Article 5a of the ZDIJZ explicitly refers to the Bank of Slovenia, the authority responsible for securities market supervision or insurance supervision, or other supervisory body specialized in financial supervision if the supervisory process in ongoing. Audit companies are not considered as "other supervisory body" as they do not perform "authoritative, public-law supervision tasks", which is the aim of this exception. As other exceptions did not apply either, the Information Commissioner decided that the applicant's appeal was well founded.

KEYWORDS: personal data, the media, decision number 090-277/2017

Reasons for denying access to documents from pending criminal procedure

The applicant requested from the Prosecutor General's Office access to final decisions to initiate investigations against certain natural persons. The body denied access due to the protection of criminal prosecution under Article 6, Para. 1, Point 6 of the ZDIJZ. The Information Commissioner concluded that criminal prosecution was still pending in all the cases at hand and that publicly revealing the requested decisions would prevent certain investigative tasks from being conducted (including hearing of witnesses), which could cause irreparable damage to the prosecution. The authorities were still gathering evidence in these cases and not all witnesses have been heard and not all other evidence have been assessed. Partial access to the requested documents was not possible and the Information Commissioner also concluded that there was no public interest in disclosure. It is important to consider the time factor when conducting the public interest test; namely, the proceedings at issue were all still pending, and the crime was still being investigated and evidence was still being gathered. According to the settled case law, the fact that a case gained high-visibility in the media is not sufficient for the public interest in disclosure to prevail, but certain values, such as life, health or safety of the people and the like, need to be threatened for there to be a public interest in disclosure.

KEYWORDS: criminal prosecution, decision number 090-307/2017

Access to complete and full information is a condition for participating in a public debate

The applicant requested from the Ministry of Economic Development and Technology access to the Agreement on the Strategic Investment Implementation signed by the state, the Municipality of Hoče-Slivnica and Magna Steyr. The body liable denied access to the document by referring to the exception of trade secret in accordance with Article 6, Para. 1, Point 2 of the ZDIJZ, which was invoked by the intervener. The Information Commissioner found that the Agreement at issue was marked as a business secret in accordance with the subjective criteria, but that there was a prevailing public interest in disclosure, so the body should grant access to the requested document. The strategic investment, which was the subject of the Agreement, was not only the subject of media attention, but also raised a number of issues and dilemmas in the local community and the general public, as for example, whether the conclusion of the requested Agreement was transparent and efficient in terms of the use of public funds; what are the Contracting Parties' rights and obligations under the Agreement in question; what will be the impact of the investment on the environment and, consequently, on human health and the quality of their life; what will be the financial effect on the country or the municipality. In order for the public to participate in an open public debate regarding the strategic investment in question, it must have the right to complete and full information, including the information from the requested Agreement.

KEYWORDS: trade secret, public interest test, decision number 090-7/2018

Public interest prevails over the interests and benefits of the public institute
The applicant requested from the Ljubljana Pharmacy, public institute, the Strategic Plan for the period 2018-2022. The body liable denied access on the grounds of the exception of the protection of business secrecy pursuant to Article 6, Paragraph 1, Point 2 of the ZDIJZ. The Information Commissioner noted that the content of the document does not concern the organisation's marketing activity but the entirety of the body itself. As the performance of public service is in the public interest, the public oversight is of utmost importance. Above all, the interests and benefits of a public institute are limited when it comes to performing public service. The Commissioner concluded that there is also a public interest in disclosing the requested document. The public has an absolute right to get acquainted with the strategic plan for the development of the largest public institute, providing medicines for treatment and products increasing the effectiveness of treatments and preservation of health. Thus, the Information Commissioner instructed the body to provide the applicant with the entire requested document.

KEY WORDS: business secret, public interest test, decision number 090-118/2018

Bodies interpret the exception of confidentiality of a source all too broadly
The applicant requested from the Inspectorate for Education and Sport of the Republic of Slovenia all information in its possession relating to a particular public institution. The liable body partially denied access to the requested document by invoking exceptions of personal data protection, confidentiality of the source of an application, protection of internal operations, protection of business secrecy, protection of the document in the process being drawn up and protection of administrative procedure. The body granted partial access and provided the applicant with 258 pages of documents, deemed freely accessible information. With regard to the exception of protection of administrative procedure, the Information Commissioner noted that the body did not consider each document individually, it did not specify what stage the administrative procedures was in, nor did it explain how disclosing each individual document would influence or harm the implementation of the specific administrative procedure. With regard to exception of confidentiality of a source, the Information Commissioner noted that this exception protects the identity of the source during the inspection procedure and not the data or communications provided by that source. Such information enjoys protection from disclosure only if it is a business secret or another type of protected information. In the case at hand, the identity of the source could be protected by redacting it from the document, thus preventing the identity of a specific individual from being discovered. This was possible as there was not so much personal information in the document to enable the identity of the source to be discovered.

KEYWORDS: administrative procedure, confidentiality of a source, decision number 090-155/2018

No general decisions when considering the public interest
The applicant requested access to the list of individuals who were naturalized in an extraordinary procedure in the period from 2007 until the date of the request, invoking, inter alia, the prevailing public interest in disclosure. The liable body denied access to the list of 3,979 individuals, relying on the exception of personal data protection and arguing that there was no prevailing public interest in disclosure. The Information Commissioner noted that its decision of 2012 concerning the extraordinary naturalization of a particular individual could not be directly referred to in this case. The previous Commissioner's decision does not automatically mean that all the names and surnames from the citizenship register of individuals that were extraordinary naturalized are freely available. Namely, if there was an overriding public interest for the disclosure in one case, this does not mean such a decision is general and applies to all similar information or information of the same type. In the case at hand, there should be an overriding public interest for the disclosure of data of each of the 3979 individuals. In demonstrating the public interest, the applicant claimed that there were doubts as to the proper conduct of the proceedings, but the Commissioner ascertained that this cannot constitute a sufficient legal basis for disclosing the names of 3979 individuals. Thus, after the Information Commissioner performed the proportionality test, the applicant's complaint was rejected as unfounded.

KEYWORDS: personal information, public interest test, decision number 090-139/2018

Soil analyses as environmental data should be absolutely public

The Society for the Environment and Nature (Društvo za okolje in naravo) requested from the Chamber of Agriculture and Forestry of Slovenia all soil analyses from the farm that was suspected of harmful emissions into the soil which could represent a threat to the groundwater. The body liable denied access to the requested documents claiming it did not possess them or, to put it differently, they are not public information as they do not arise from it performing a public service but from its market activities. The body noted that it does not own or manage the computer application in which it enters data and documents, including the requested ones. The application is managed by the Agency of the RS for Agricultural Markets and Rural Development, which means that the body liable does not have any authority to provide the requested documents. The Information Commissioner did not accept such argumentation and, contrary to this position, found that the body possessed the documents and that they are public information. Likewise, the Information Commissioner did not follow the liable body's position that the soil analyses and fertilization plans which the body obtained against payment on the market were the result of pursuing a purely market activity and not part of its public service. The Information Commissioner further noted that the requested data is environmental data and as such absolutely public in line with the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters. The Information Commissioner thus upheld the applicant's appeal and ordered the body to provide the applicant with all the requested soil analyses, including the farmer's first and last name.

KEYWORDS: environmental data, personal data, decision number 090-128/2018

Unpublished copyright material can also be a business secret

The applicant requested from public institute Auditorium Portorož access to documents related to a call for tender of the 38th festival Melodies of the Sea and Sun, Portorož 2018, including a list of all applications received, notes on any eliminations of the applications from the process, sound recordings of songs, the methodology of song selection and evaluation methods, etc. The body liable denied access relying on personal data protection exception. However, the Information Commissioner concluded that the names and surnames of the applicants of the selected songs ought to be public because they are information related to the use of public funds. The call for tender explicitly stated that (monetary) prizes shall be awarded at the festival and the applicants themselves who have been selected to participate in the festival shall receive a gross amount of EUR 400.00. However, personal data of the applicants who submitted songs that were then not selected should not be made public as there is no legal basis for that. Furthermore, all information relating to the selected songs (namely, the title, artists and sound recordings) is public information as it relates to the use of public funds. The Information Commissioner finally noted that information about the songs that were not selected (namely, the title, artists and sound recordings) are the applicants' business secrets. As the applicants were only allowed to submit material that had not yet been broadcasted to the public, the disclosure of such materials in the present proceedings would cause significant damage to the parties concerned.

KEY WORDS: personal data, business secret, decision number 090-172/2018

Procedures of treating foreigners at the national border are not internal operations of the police

Amnesty International Slovenia requested from the Police access to instructions and guidance on the conduct of the police on the ground in the context of increased migratory pressures. The body relied on the exception of internal operations of the body and personal data protection. While the disclosure of names of civil servants is usually not questionable, the disclosure of personal data of seconded civil servants in cases such as the one at hand could cause disturbances in operations of the body. The public could infer from the civil servants' names the number of staff seconded to protect the national border and the areas where the police presence will be lower as a consequence, which could reduce the efficiency and effectiveness of the police's operational work. The requested documents also contain operational information, extracted from the risk analysis of cross-border crime and irregular migrations. Disclosure of operational information and operating tactics could cause immediate deterioration of security situation. The Information Commissioner partially upheld the complaint as it found that the body did not demonstrate any disturbances to its operation that would result from disclosure of the requested documents. Moreover, the Commissioner concluded that there was prevailing public interest for the disclosure. Namely, the Commissioner confirmed the applicant's position that the public has the right to know whether the police implements border procedures lawfully, uniformly, predictably and within the statutory powers conferred on them. Each individual who becomes a subject of police procedures has the right to know how these procedures are conducted, what rights does

he/she have etc.
KEYWORDS: internal operations of the body, public interest test, decision number 090-223/2018

Procedures of treating foreigners at the national border are not internal operations of the police
Amnesty International Slovenia requested from the Police access to instructions and guidance on the conduct of the police on the ground in the context of increased migratory pressures. The body relied on the exception of internal operations of the body and personal data protection. While the disclosure of names of civil servants is usually not questionable, the disclosure of personal data of seconded civil servants in cases such as the one at hand could cause disturbances in operations of the body. The public could infer from the civil servants' names the number of staff seconded to protect the national border and the areas where the police presence will be lower as a consequence, which could reduce the efficiency and effectiveness of the police's operational work. The requested documents also contain operational information, extracted from the risk analysis of cross-border crime and irregular migrations. Disclosure of operational information and operating tactics could cause immediate deterioration of security situation. The Information Commissioner partially upheld the complaint as it found that the body did not demonstrate any disturbances to its operation that would result from disclosure of the requested documents. Moreover, the Commissioner concluded that there was prevailing public interest for the disclosure. Namely, the Commissioner confirmed the applicant's position that the public has the right to know whether the police implements border procedures lawfully, uniformly, predictably and within the statutory powers conferred on them. Each individual who becomes a subject of police procedures has the right to know how these procedures are conducted, what rights does he/she have etc.

KEYWORDS: internal operations of the body, public interest test, decision number 090-223/2018

2.4 GENERAL ASSESSMENT AND RECOMMENDATIONS IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

In 2018, the Information Commissioner celebrated the 15th anniversary of the entry onto force of the Public Access to Information Act. In 2003, when the law came into force, it was impossible to predict the impact the law will have on the functioning of public sector bodies. The law brought about a complete change of the system; from one in which almost no information was publicly available to a system of complete openness, where only the law may provide for exceptions to free access and the principle of transparency is one of the guiding principles of functioning of the public sector.

As in the past few years, the Information Commissioner also identified some positive indicators in 2018: on the one hand, the applicants are increasingly aware of their right to access to public information and, on the other, bodies liable respond more frequently to the applicants' requests. The upward trend in the number of complaints received over the last few years continued in 2018, which means that the applicants are well acquainted with their right to the legal remedy and are keen to use it. The complaints procedure is entirely free of charge and relatively swift for the applicants. Thus, the Information Commissioner considers that the complaints procedure provides an effective legal protection of the right to access to public information. In 2018, the Information Commissioner additionally reduced the average time of resolving the complaints, which has now settled at 32 days (to offer a comparison: in 2017 the average time was 37 days and in 2016 47 days). It should be noted that in accordance with the General Administrative Procedure Act (ZUP) the statutory time-limit in such matters is two months.

The Information Commissioner received numerous requests for opinions and positions in 2018 as well, and it provided these in the context of its informal counselling on the basis of its established practice. This shows that throughout this year the bodies liable have been active and responsive and often asked turned to the Information Commissioner even outside complaints procedures, i.e. even when not prompted by a legal requirement. A relatively low number of administrative disputes brought against the Information Commissioner's decisions point to the fact that the bodies liable are willing to cooperate with the Information Commissioner and follow its recommendations. In 2018, only 11,8 % of Commissioner's decisions were challenged before the Administrative Court. The Information Commissioner regularly publishes its decisions on the website, trying to make its practice available in a transparent and timely manner in order to facilitate the work of the bodies liable and to inform the public of the importance of this fundamental human right as effectively as possible.

Nevertheless, the Information Commissioner considers the cooperation with bodies liable exemplary (in 2018, it did not initiate any minor offence proceedings in accordance with ZDIJZ, ZInfP or ZMed). However, it still notes two trends: 1) that the number of complaints against the so-called administrative silence again rose this year and 2) that the number of complaints against municipalities increased after the trend was already downward before 2017. The rise in the number of complaints cannot be fully contributed to the lack of response of the bodies; the fact is also that there has been an increase in the number of requests made to the first instance bodies and also that many ambiguous requests have been filed, namely such that could be handled on several different legal bases (not only in accordance with ZDIJZ but also in accordance with the procedural legislation giving rights to the party to the proceedings, the complainant, the municipal councillor etc.). In such cases there is a question of which legal basis the body should use to conduct the proceedings, which may lead to (unfounded) complaints procedures before the Information Commissioner.

In 2018, the Information Commissioner handled 21 complaints against business entities subject to dominant influence of entities of public law. While the number increased compared to the previous year, it still accounts for a relatively small share (3.8%) of all complaints (549) handled by the Information Commissioner.

With regard to the re-use, the Information Commissioner conducted one complaint procedure in 2018. The Information Commissioner estimates that the applicants, i.e. potential re-users, are well aware of their legal options when faced with a refusal decision, but they do not often decide to use the complaint procedure. Since the entry into force of the amendment ZDIJZ-E, the principle of proactive publication of information applies in the field of re-use of public information. In practice, this principle is implemented through the publication of information through the OPSI Open Data Portal managed by the Ministry of Public Administration. In this way, the potential re-users can obtain such open data swiftly and without special procedural requirements, to which the Information Commissioner is bound in the complaints procedure under the ZDIJZ and ZUP.

Basing its observations on the specific complaint cases, the Information Commissioner makes the following findings and recommendations for the further work of liable bodies:

I. The bodies liable should pay more attention to procedural issues when handling the requests, in particular to substantiating rejection decisions. If a body denies the applicant's request for access relying on statutory exceptions, it is crucial to fully establish and describe the actual situation and to consider the content of the required documents in detail. It must be clear from the statement of reasons which documents were considered and which parts of applicant's request were rejected. The reasons for the rejection must be explained in a way that the applicant understands it and that they are consistent with the operative part of the decision. In 2018, the Information Commissioner noted an increase in the number of complaints filed for the breach of procedural rules due to inadequate statement of reasons, which also had an effect on the applicants' right to an effective remedy.

II. With regard to the exceptions relied upon in the proceedings by the bodies liable, it should be noted that the number of complaints where the exception of internal operations was relied upon. The Information Commissioner concludes that the bodies interpret this exception too broadly and without specifically demonstrating the harm that would result from the disclosure of the requested documents. The Information Commissioner pointed out that this exception cannot be applied to every document of internal nature, but is usually applied to various internal instructions, notes and work plans. It follows from the principle of free access laid down in Article 5 of the ZDIJZ that the body may deny access to information only if it proves the existence of the alleged exception. In other words, the burden of proof lies with the body, and if the burden is not met, the information should be considered freely accessible.

III. In 2018 the Information Commissioner handled a few complaints where the bodies liable denied access to information related to the execution of employment relationship of public servants on the grounds of personal data protection. In this regard it should be pointed out that the legal basis for providing such information to the public has not changed even after the entry into force of the GDPR. Namely, the provision of Article 6, Para. 3 of the ZDIJZ defines such information as absolutely public and this was incorporated into the established practice of the Information Commissioner and case-law of the Administrative Court.

IV. In its practice, the Information Commissioner also identified several cases in which bodies liable, who found the existence of a statutory exception, denied access completely instead of allowing partial access to information in accordance with Article 7 of the ZDIJZ. In this regard it should be noted that if the document

or part of a document contains only a part of the protected information, which may be excluded from the document without jeopardizing its confidentiality, the body shall apply the rule on partial access and enable access to the rest of the document, which is not protected, to the applicant.

V. With regard to the finding referred to in the previous paragraph, there is an increase in the number of cases regarding access to documents from inspection procedures. Therefore the Information Commissioner notes that the rule on partial access also applies to reports in inspection procedures and other documents from these procedures, which are not protected absolutely and entirely, but only parts of such documents are protected if they contain a statutory exception (e.g. the body should protect personal data, information on the applicant etc. and not the complete report, including in case of an anonymous report).

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 has been the Personal Data Protection Act (ZVOP-1).

The development of modern information and communication technologies has brought about the need to adapt and update the legislative framework at 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 the 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 the 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 has not yet been adopted by the end of 2018.

3.2 INSPECTION SUPERVISION IN 2018

Due to the suspicion of violations of the provisions of the ZVOP-1, in 2018 the Information Commissioner conducted 1,029 cases of inspection, of which 330 pertained to the public sector and 699 to the private sector. In comparison to the previous year, this represent a 57% increase in inspection procedures. On the basis of complaints against public sector legal entities it initiated 279 inspection procedures, while it initiated 51 procedures ex officio; furthermore, it initiated 660 inspection procedures on the basis of complaints against the private sector, while it initiated 39 procedures ex officio. Within the framework of inspection procedures, 22 on-site inspections were carried out in the public sector and 81 in the private sector.

With regard to complaints, the largest number of suspected violations of the provisions of the 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 (269 cases);
- Abuse of personal data for direct marketing purposes (171 cases);
- Unlawfully collecting or requiring personal data (138 cases);
- Unlawful video surveillance (97 cases);
- Inadequate security of personal data (69 cases);
- Unlawful access to personal data (58 cases);
- Processing personal data contrary to the purposes for which they were collected (49 cases);
- Other (49 cases).

In order to redress the established irregularities, the Information Commissioner issued a total of 59 measures (17 in the public and 42 in the private sector) in the form of warnings on the record, preliminary decisions and regulatory decisions.

Due to violations of the provisions of the ZVOP-1, **101 minor offence proceedings** were initiated in 2018 (105 in 2017 and 83 in 2016), of which 42 were against legal persons from the public sector and their responsible persons and 31 were against legal entities in the private sector and their responsible persons. 28 proceedings were against individuals.

In minor offence proceedings, including those initiated in the previous years, the Information Commissioner issued 9 warnings and rendered 42 minor offence decisions (20 fines and 22 cautions). Furthermore, the Information Commissioner issued 42 additional warnings for minor violations, which is in line with the principle of procedural economy. In response, the suspected offenders filed a total of seven requests for

judicial protection.

In 2018, the Information Commissioner received a total of eight decisions of the local courts on requests for judicial review pertaining to this and past year's decisions. In two of those cases the court reduced the imposed fine, in four it dismissed the request for judicial review as unfunded and in two the proceedings were stayed.

The Information Commissioner also received a judgment of the Supreme Court of the Republic of Slovenia on the request for the protection of legality, filed by the State Prosecutor General at the initiative of the offender against the decision of the District Court regarding the decision of the Information Commissioner.

COOPERATION IN CROSS-BORDER INSPECTION PROCEDURES

In the period from the entry into force of the GDPR, i.e. 25 May 2018, until the end of the year, the Information Commissioner identified itself as the supervisory authority concerned in **81 procedures of identifying the lead supervisory authority** for the cross-border supervision under Article 56 of the GDPR. On the basis of the aforementioned procedures of identifying the lead supervisory authority, **30 procedures of cross-border cooperation in supervisions** were initiated against companies with cross-border activities on the basis of the "one-stop-shop" mechanism (Article 60 of the GDPR), in which the Information Commissioner participates as the supervisory authority concerned. In 2018, none of the procedures were completed; for the most part, they were still in the process of consultation between the authorities.
The Information Commissioner participated in **6 mutual assistance procedures** under Article 61 of the General Regulation.
For the most part, the Information Commissioner cooperates in cross-border supervisions when they concern top multinational internet corporations, such as Facebook, Google, Twitter, LinkedIn, Amazon, Apple, etc., and the compliance of their practices with the GDPR.

SELECTED CASES OF PROCESSING OF PERSONAL DATA

Direct marketing and individual rights
The Information Commissioner receives a large number of reports about the adds individuals receive without their consent. Usually, the Information Commissioner does not initiate an inspection procedure in such cases, because the consent of the individual is only one of the possible legal bases, while with direct marketing one should also consider legitimate interest of the controller as a possible legal basis. Individuals can ask the controller where it obtained their personal data and whether there is a legal basis for the processing by means of a request to access his/her personal data (Article 15 of the GDPR). An individual may also object to the processing of personal data by the controller at any time (Article 21 of the GDPR) and may also exercise the right to erasure of personal data (Article 17 of the GDPR, i.e. the right to be forgotten). The individual may also request from the controller the termination of personal data processing for direct marketing purposes in writing or in another agreed manner on the basis of Article 73 of ZVOP-1, which stipulates that the data controller shall be obliged within 15 days to prevent the use of personal data for the purpose of direct marketing, and within the subsequent 5 days to inform in writing or another agreed manner the individual who so requested.

Taking photographs of children at school and kindergarten events
The Information Commissioner received numerous questions of concerned parents, primary schools and kindergartens whether taking photographs of children's performances is allowed or not. Thereupon, the Commissioner issued a press release, emphasizing that the GDPR does not prohibit parents from photographing their own child at Christmas performances or other events. Parents who take photographs or record their children usually process personal data for their own personal use, namely for private purposes. Parents, however, should be careful not to share other children's photographs with third parties, in particular on the Internet and social media without their parents' consent. However, if the school or kindergarten is recording or taking photographs, there must be a proper legal basis for such processing. Since the law does not provide such a legal basis, the only possible legal basis for processing is the personal consent of parents or other legal representatives. Only photographs and recordings that do not interfere with the children's privacy may be published. However, in the case of a public event, the organizer is not obliged to obtain special personal consents for general photographing of the event and publication of material, if the participants are appropriately informed in advanced about photographing / recording and publication of the materials (i.e.

provides information in accordance with Article 13 of the GDPR). Individuals attending a public event ought to be aware that such an event is more likely to be recorded / photographed and that the materials might be published in various media for the purpose of presentation of the event itself.

Processing of personal data upon joining a trade union and for the purpose of calculating membership fees
Information on trade union membership is considered special type of personal data (according to the terminology of ZVOP-1: sensitive personal data). Article 9 (2) (d) of the GDPR constitutes a direct legal basis for the processing of personal data of trade union members, providing that the processing of personal data is legal if the processing is carried out by trade unions in the course of their legitimate activities with appropriate safeguards, on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects. The trade unions therefore do not require personal consent for processing of personal data for the purposes of concluding a membership and pursuing legitimate trade union activities. They are only required to give the individuals adequate information on all processing information (Article 13 of the General Regulation). The employee can pay union membership directly to the union or through the employer at the payroll. In such a case, the employer is nor the controller nor the processor of the union, but the user of such data. If both methods of payment are possible, the union must obtain proper authorisation of its members to pay the membership fee through the employer. However, if payment of the membership fee is only possible through the employer, the trade union must inform the individual and provide the types of personal data that it will transmit to the employer for this purpose.

Banks processing personal data of family members of a potential borrower from the central credit register
The Information Commissioner received several complaints against banks for obtaining personal data from the central credit register for family members (especially partners) of potential borrowers. The Information Commissioner concluded that neither the Consumer Credit Act nor the Central Credit Register Act provide banks with a legal basis for obtaining personal data from the central credit register of anyone other than the borrower. The banks cannot even obtain personal data from the register on the basis of the individual's the consent, because the Bank of Slovenia, who established and manages the central credit register, is a part of the public sector, and personal data in the public sector can only be processed if so prescribed by statute. Personal consent may only be a legal basis if this is allowed by a statute, which is not the case here. The bank could obtain personal data of partners or other family members of potential borrowers from the central credit register from data subjects themselves who would exercise their right to access to their personal data. However, upon the request of such personal data, the bank should provide the potential borrower and his / her family members with concise, transparent and easy to understand information as referred to in Article 13 of the GDPR.

Video surveillance of work areas and monitoring of live image
Video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means. Special attention is needed in regulating access rights to video surveillance systems and granting access to the live image. Monitoring of live image should only be allowed for the safety of people or property and when this purpose can be achieved by the very nature of things only by continuous monitoring of the live image during the work process (not by occasional, random access) by authorized persons, e.g. a security guard, not a person authorized to supervise the worker discharging his/her obligations. This is because the likelihood that an incident will occur at the very moment when the manager or another supervisor randomly accesses the video surveillance system is negligible, which makes the monitoring of live images by managers unfounded. Employers must designate and authorise persons with access to the video archive, and in exceptional cases, persons who will monitor the live image in accordance with the legitimate purposes of video surveillance. Access to the video archive or monitoring a live image solely for the purpose of monitoring employees constitutes a violation of the provisions of the ZVOP-1.

Unlawful access to health data and obtaining information on individuals who accessed it

The Information Commissioner initiates an inspection procedure for alleged unlawful access to health data only if the applicant gives concrete reasons for suspecting (not merely alleging) that the employees of a particular controller illegally accessed his / her personal information. If the suspicion of unlawful access to health data is confirmed, the Information Commissioner, as a rule, imposes a fine on the offender. Some individuals whose names appeared in access logs attempt to avoid liability by claiming that they did not access the data themselves but that someone else was using their password. In such cases too will the Information Commissioner fine the offenders, not for the unlawful processing of personal data, but for the inadequate security of passwords, since unknown persons used their passwords to process the patient's personal data without authorization and legal basis. If employees do not log out of the system and several people can use the same password, there is no proper internal traceability of processing of personal data as one of the measures for securing personal data, essential for detecting unauthorized access to personal data.

Processing of personal data of members of societies

The Information Commissioner takes the view that membership in a society constitutes a contractual relationship, because the member, by concluding the membership, agrees to certain obligations and acquires certain rights regarding his / her participation in the society. Therefore, the processing of personal data of members of a society is lawful if necessary for the performance of the contract. A possible legal basis for the processing of personal data of members of the society may also be the legitimate interests pursued by the controller, whereby the society must provide the individual with concise, transparent, understandable and easily accessible information about the processing of the data. Personal consent as the basis for the processing of personal data of members of societies is therefore less frequently used, but is a possible basis in particular in situations when processing personal data for purposes other than those directly related to the operation of the society, especially in the case of the transfer of personal data to third parties (e.g. publication on the society's website). In accordance with the GDPR, the consent must be concrete, informed and comprehensible declaration made with clear affirmative act and demonstrable. Therefore, members' consents which referred to general terms and conditions of processing within the society's internal acts and were obtained prior to the entry into force of the GDPR, are no longer relevant. Societies should therefore obtain new consents for the processing of personal data that is not necessary for implementing the society's basic activities.

Supervision of multinational providers of advanced communications services

The business model of online service providers, social networks and communication platforms (Facebook, Google, Instagram, Twitter, WhatsApp, Viber, etc.) is most often based on a service that is free to the user but monetized through personalized and targeted advertising based on processing vast quantity of personal data. Often, these practices are invisible and insufficiently communicated to the individual. The GDPR brings many novelties to these technological giants, including a substantially broader territorial scope of the GDPR, which included these companies under the GDPR wing, stricter provisions on profiling, information for data subjects and exercising their rights, and greater accountability of companies for advance data protection impact assessment of the effects of data processing on the data subject. The supervisory authorities have also been given stronger tools to supervise these controllers, notably in terms of improved operational cooperation between the supervisory authorities for the protection of personal data based on the principle of "one-stop-shop" mechanism.

3.3 OTHER ADMINISTRATIVE PROCEDURES

Implementation of biometric measures
The Information Commissioner received 4 requests for the implementation of biometric measures and issued 6 decisions on the permissibility of such measures. It allowed two controllers to implement biometric measures with the use of fingerprint scanner, namely for entering a secure system room where core business-technical infrastructure and information-communication hub, and for entering the chamber (the so-called "clean space"), in which drugs for autologous cellular therapy are prepared. It rejected the applications of four controllers requesting permission to implement biometric measures to record working hours and / or to unlock doors.

Connecting filing systems
In 2018, the Information Commissioner permitted 10 data controllers to connect personal data filing systems. Among others, it allowed the Slovenian Maritime Administration to connect its Sea boats Register with the Central Residential Register managed by the Ministry of the Interior; the Employment Service of Slovenia to connect its Unemployed persons Register with the Business Register of Slovenia, managed by the Agency of the Republic of Slovenia for Public Legal Records and Related Services; and it allowed the Financial Administration of the RS to connect its Inheritance and gift tax assessment Register with the Real Estate Register, managed by the Surveying and Mapping Authority of the Republic of Slovenia.

Transfer of personal data – until 24 May 2018
In 2018, the Information Commissioner received 12 applications for the transfer of personal data out of the Republic of Slovenia, 8 of which have been filed until 24 May 2018. Until this date the Information Commissioner issued 12 decisions by which it permitted 10 companies to transfer personal data, mostly to the United States and Serbia, but also to Israel, New Zealand and India. Three companies were allowed to transfer personal data to affiliated companies within the international group of companies.

Transfer of personal data under the GDPR – from 25 May 2018
The permission of the Information Commissioner to transfer data to third countries or international organizations is in accordance with the GDPR in most cases no longer required. In some cases, however, it is still necessary to obtain a permission, namely a decision, as to the adequacy of the safeguards referred to in Article 46 of the GDPR which form the basis for the transfer of data. As of 25 May 2018, no decisions have been issued by the Information Commissioner. However, it issued six procedural decisions terminating the proceedings, namely one decision to stay the proceedings and five decisions to dismiss the proceedings for lack of jurisdiction, as it no longer has the authority to issue the decisions on adequate levels of personal data protection requested by the applicants.
In December 2018, the Information Commissioner issued revised guidelines on data transfers setting out the details with regard to transferring personal data to third countries and international organizations under the GDPR.

Data subject's rights
In 2018, the Information Commissioner received 106 appeals regarding the right of the individual to access to personal data (a few less than in 2017, when it received 110 appeals). 56 appeals filed concerned public sector controllers and 50 appeals controllers from the private sector. Before 25 May 2018, there 40 complaints were filed, while after that date there 66 complaints were filed, some of which related to the law in use before 25 May 2018. In 106 appeal procedures, which are governed by the General Administrative Procedure Act, the Information Commissioner issued 19 administrative decisions (which is 73% more than in 2017) and in the rest of the appeal procedures, after the declaratory proceedings, it issued 68 decisions, formal explanations, calls and proposals to act. Most decisions were favourable to individuals.

3.4 OPINIONS AND CLARIFICATIONS

General clarifications

In 2018, the Information Commissioner issued 2,192 written opinions and referrals to the already published opinions, which represents a 70% increase in comparing to the previous year. **Around 4,000 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 giving advice and answers to questions over the telephone. Thus, a Data Protection Supervisor is on duty every day to answer such calls over the telephone. **In 2018, state supervisors received 3.230 calls, while there were 1.998 such calls in 2017, which is an almost 62% increase in the number of calls.**

Participation in the preparation of laws and other regulations

The Information Commissioner issues opinions to regulations in accordance with the provisions of Article 57(c) of the GDPR and Article 48 of ZVOP-1. **In 2018, the Information Commissioner issued 60 opinions on proposed amendments to legislation and on proposed new laws and regulations**. A positive trend is seen for the first time in years, namely that the number of regulations that affect the privacy of individuals in terms of the processing of personal data has decreased significantly, as the Information Commissioner issued almost double the number of such opinions in 2017.

3.5 COMPLIANCE AND PREVENTION

In 2018, 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
The Commissioner issued guidelines on contractual processing with the aim of explaining the controllers, with practical examples, what contractual processing is, what are the obligations of data controllers and processors, the pitfalls and recommendations for complying with the regulation on outsourcing services when it includes personal data.

Records of processing activities
In order to assist the liable entities in establishing the records of processing activities, the Commissioner published on its website a description of duties with explanation and instructions. The Commissioner also prepared two templates of records of processing activities (template for controllers and template for processors) so that liable entities can easily and efficiently register their personal data filing systems.

Data breach notification
To assist the controllers with their data breach notifications, the Information Commissioner in cooperation with employees from the inspection area of competence, designed an appropriate breach notification procedure and created a dedicated mailbox (prijava-krsitev@ip-rs.si). The Commissioner also prepared internal instructions on how to deal with the notifications received (including in cross-border cases), while at the EU level a template on security breach notifications was created and is available on the Information Commissioner's website.

Personal data impact assessments
The Information Commissioner prepared and published detailed explanations and practical guidelines for liable entities on conducting personal data impact assessment, with a sample methodology, recommendations and numerous examples. The Information Commissioner established a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and communicated the list to the European Data Protection Board for confirmation.
Where the data protection impact assessment indicates that the processing would result in an unacceptably high risk, the controller shall consult the supervisory authority prior to processing. In 2018, the Information

Commissioner issued six opinions on data protection impact assessments that it received for prior consultation.

Data protection officers
In 2018, the Information Commissioner carried out a number of activities related to data protection officers, namely it:

- Provided detailed explanations with links to useful materials on its website,
- Prepare and publish a form for designating data protection officers,
- Set up an internal process to handle and manage the designation forms received, including the acknowledgement of designation and a warning in the event of an apparent conflict of interest,
- Issued recommendations on the activities of the data protection officer with a sample of the annual work plan of the data protection officer.

By the end of 2018, **1920 liable entities reported the designation of the 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.

Codes of conduct and certification
In 2018, the Information Commissioner received only one draft code of conduct that was not yet eligible for approval. 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 possibility still requires the development of appropriate accreditation and certification systems; activities are still ongoing at the EU level and so certification was not possible in any Member State in 2018.

Training and awareness raising activities
The Information Commissioner has significantly strengthened its training and awareness raising activities in 2018.

After substantially restructuring its website (www.ip-rs.si), the Commissioner started publishing updates on the adoption of the GDPR, outlining key areas of the Regulation and adding to the existing content, all due to the adoption of the GDPR.

The Information Commissioner also prepared different **materials**, namely:

- Guidelines: Guidelines on contractual processing, Guidelines on personal data protection impact assessments, Guidelines on the transfer of personal data to third countries and international organizations, Guidelines on personal data protection statements for websites, Code of conduct for the collection of personal data, guidelines Informed consumers – to whom do we hand out our personal data and why;
- Forms: Sample form for recording processing activities (for controllers and processors), Sample form for information to be provided to data subjects pursuant to Articles 13 and 14 of the GDPR, Recommendations on the activities of data protection officers with a sample of the data protection officers' annual work plan, Form for designating data protection officers, Form for data breach notification;
- Infographics that present certain thematic areas, which are very complex, in a simple and effective way: Infographics on legal bases for the public sector, Infographics on legal bases for the private sector with a valid consent, direct marketing.

The Information Commissioner also **organized and conducted numerous events**. On the occasion of the European Data Protection Day, it organized a special event on GDPR and presented awards for good practices in the public and private sectors, a special award Ambassador of privacy and awards to the recipients of the information security management certificate ISO/EIC 27001: 2013. The 2017 Privacy Ambassador Award went to the ICS - Institute for Corporate Security Studies. In 2018, the Information Commissioner delivered 109 pro bono lectures on the novelties of the GDPR to various chambers and associations in the public and the private sector and at conferences and seminars.

The Information Commissioner also participates in various projects. At the end of 2018, it launched 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. It is co-financed by the European Union as part of the Rights, Equality and Citizenship Programme 2014-2020 and will last until September 2020. In the first part of the project, aimed at enterprises, a new website **www.upravljavec.si** was set up, containing explanations, guidelines and forms to help the controllers with the fulfilment of legal requirements in the field of personal data protection; a telephone consultancy was set up at a toll-free number; and the Information Commissioner will carry out 20 lectures free of charge in cooperation with the Chamber of Crafts and Small Enterprises of Slovenia and the Chamber of Commerce and Industry of Slovenia. The second part of the project is intended to educate individuals on the importance of privacy and their fundamental rights in the field of personal data protection. For this purpose, the Commissioner established a new website **www.tiodlocas.si** aimed at individuals and focusing on their rights. In 2019, the Commissioner will cooperate with the Slovenian Consumers' Association and will prepare an occasional piece for the ZPSTest magazine. It will also continue to actively participate in the Council of the SAFE-SI Project and the Web Eye, which carry out important preventative activities on internet safety for pupils, teachers and parents.

The Information Commissioner also strengthened its **presence on social networks**. Thus, it established a presence on the professional LinkedIn network with the aim of reaching out to business users. It has also strengthened its communication on its Facebook page, aiming at raising awareness of the general public on privacy issues in relation to the use of web related services.

3.6. GENERAL ASSESSMENT OF THE STATE OF PERSONAL DATA PROTECTION

The activities of the Information Commissioner in the field of personal data protection in 2018 were largely marked by the GDPR, which became directly applicable in all EU Member States on 25 May 2018 and expanded the Information Commissioner's duties and responsibilities in comparison to the existing ZVOP-1. The new requirements put forward by the GDPR considerably increased the scope of controllers' and Information Commissioner's activities in the field of personal data protection.

With the entry into force of the GDPR the adoption of a new Personal Data Protection Act (ZVOP-2) is required in Slovenia to ensure the complete implementation of the said Regulation. Such a law was not adopted by the end of 2018, which caused many uncertainties for data controllers, data processors and the Information Commissioner. The fact that ZVOP-2 was not adopted did not have a significant impact on the conduct of inspection proceedings, but it did have a significant impact on the conduct of minor offence proceedings and the imposition of fines for the violations detected. In the inspection procedure, the Information Commissioner may, due to the absence of ZVOP-2, only order the liable entity to correct the irregularities identified and prohibit or block personal data processing in the event of violations of the GDPR or ZVOP-1. Minor offence proceedings can only be initiated for violations of those provisions of the ZVOP-1 that are still was in force. The Commissioner was thus unable to impose sanctions for violations laid down in Article 83 of the GDPR in 2018 and could only sanction the violation of those provisions of the applicable ZVOP-1, which were not replaced by the GDPR.

As in previous years, the Information Commissioner received a large number of reports from individuals in 2018, and this number further significantly increased after the entry into force of the GDPR. From 25 May 2018 to 31 December 2018, the Information Commissioner thus received 598 reports of violations of personal data protection, while in the same period of 2017 it received only 290 reports. Such a significant increase in the number of reports is undoubtedly the result of increased awareness of individuals regarding the processing of their personal data and the rights conferred on them by the GDPR, since the latter has been widely discussed in the media in the adoption phase. The awareness of the controllers and processors also increased, which led to increase numbers of requests for oral and written opinions of the Information Commissioner. Analysing the reports by individuals, the Information Commissioner found that very often they were a result of misunderstood provisions of the GDPR, which is particularly the case with processing of personal data on the basis of data subject's consent. It is true that the GDPR enacted more stringent conditions for the consent of the individual to be valid, but it should be noted that the individual's consent is only one of the six legal bases for lawful processing laid down in Article 6 of the GDPR. A poor understanding of this prompted the controllers into obtaining consent from individuals even in cases where the processing was already stipulated by law, necessary for the performance of the contract or another legal basis from Article 6 of the GDPR existed.

The Information Commissioner also notes that many reports of suspected violations were a result of the fact that controllers did not provide the individuals with relevant and complete information upon the collection of personal data. The controllers have the responsibility to take appropriate measures to provide the individual with information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The types of information which the controller is obliged to provide to the individual are laid down in Articles 13 and 14 of the GDPR, allowing the individual to learn who the controller is, for what purposes and on what legal basis personal data are processed, who are the users personal data, how long the data is stored, etc. Violations of Articles 13 and 14 of the GDPR are among the more frequently detected violations in 2018, which led the Information Commissioner to prepare and publish samples of such notices on its website.

Post offices and banks were among those who failed their obligation to provide information when collecting personal data in accordance with the EU Regulation on information accompanying transfers of funds and the Anti-Money Laundering and Terrorism Financing Act. These controllers did not provide individuals with the information collected under Article 13 of the GDPR, in particular information relating to the purpose and legal basis for the processing. This made individuals suspect that the processing is unlawful or at least excessive and they started filing reports with the Information Commissioner. Failure to provide such information constitutes a violation of the rights of the individual referred to in Article 13 of the GDPR; after the adoption of the ZVOP-2 it will be possible to impose fines for such violations set out in Article 83 (4) of the GDPR.

In the period from 25 May 2018 to 31 December 2018, the Information Commissioner also received 68 data breaches notifications sent by data controllers. The obligation to send such notifications (self-reported breaches) is a novelty imposed by Article 33 of the GDPR upon the controllers and processors. As it seems thus far, controllers have been quite diligent in reporting security incidents to the Information Commissioner by way of data breach notifications. Most frequently, data breach notifications were sent for unjustified disclosure of personal data (disclosure of personal data to unauthorized or wrong persons), unauthorized access to personal data (due to a software error or a misuse of powers by the employees), hacking into the information system, and loss or theft of personal data carriers (e.g. personal computers and office mobile phones).

In 2018, the Information Commissioner increased its efforts to perform the so-called “preventive inspections” of liable entities in areas where, according to the risk assessment, there is a greater likelihood of violations or, due to the increased sensitivity of personal data, there is a greater risk of major adverse consequences for individuals in the event of a violation. During the more comprehensive inspections, the Information Commissioner paid particular attention to the issue of compliance of processing with the provisions of the GDPR and to ensuring information security aimed at preventing unauthorized processing and the accidental or unauthorized destruction or loss of personal data.

Analysing the reports and carrying out preventive inspections, the Commissioner concludes that a large number of irregularities and deficiencies are due to the ignorance or misunderstandings of the legislation, namely the fact that the new GDPR came into force in 2018 and the ZVOP-2 was not yet adopted meaning a lack of full implementation and more clearly defined rules. The exception to this is security breaches that occur due to controllers’ or processors’ negligent behaviours, as well as unlawful accessing to personal data files by employees who do so either out of curiosity or for obtaining personal data for their own purposes. The Information Commissioner notes that the most common areas where employees access personal data filing systems is internal affairs, namely the police, and health sector institutions. Quite common is also unlawful access to data in the central dog register. Most of these personal data filing systems guarantee subsequent traceability of access, which means that it is possible to subsequently identify which persons have accessed the personal data of a particular individual at a certain time. While the employees with the right to access to personal data due to the nature of their work are well aware that such traceability exist, they nevertheless unlawfully access data in the hope that they will not be discovered. When employees who performed unlawful access to personal data are caught by the data controller or the Information Commissioner, they often state that they did not in fact access personal data, but rather that someone misused their username and password. This, whoever, does not relieve them of liability, as they are obliged to ensure the security of personal data kept in a particular filing system by securing their username and password and by logging out of the system immediately after they finish their work in the filing system or upon leaving the workstation.

In 2018, the Information Commissioner strengthened its activities in the area of compliance and prevention.

When the GDPR came into force it became obvious that many small controllers have poor knowledge of personal data protection legislation, which the Information Commissioner believes is largely due to the fact that they were previously exempt from the obligation to report their filing systems ("filing system catalogues"). There was also lack of knowledge on the different possible legal bases, in particular with regard to processing on the basis of consent and concluding a contract, as well as poor knowledge on direct marketing rules. Awareness raising activities aimed at small businesses, which are, after all, the backbone of the Slovenian economy, will thus need to be strengthened and small businesses will need to be provided with appropriate tools to ensure compliance (opinions, guidelines, forms, samples, infographics, telephone assistance and other content on websites). The Information Commissioner will continue to carry out numerous activities in this field within the RAPiD.Si project. In cooperation with the chambers of commerce, industry and crafts of Slovenia, the Information Commissioner will attempt to reach as many small businesses as possible with educational content and useful tools. The GDPR brought important novelties with regard to cooperation between data protection supervisory authorities in the EU and EEA Member States (Iceland, Norway and Liechtenstein) in cross-border cases. It has enabled and formalized a cooperation process on the basis of the principle of "one-stop shop", which provides that the inspection procedure in cross-border cases is led by the so-called lead authority in cooperation with other supervisory authorities; it introduced the mechanisms for mutual assistance and joint operations of supervisory authorities in EU Member States. Since the entry into force of the GDPR, the Information Commissioner has thus been involved in six mutual assistance procedures between data protection authorities in 2018. In 81 procedures of determining the lead authority, the Information Commissioner identified itself as the data protection authority concerned and thus participated in the cross-border inspection procedure of the liable entity. On the basis of these procedures, 30 cross-border cooperation procedures were initiated for the cooperation under a one-stop shop mechanism in inspections of companies who operate cross-border. In the majority of cases, these companies were popular online communication service providers, the online giants such as Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft, etc. The Information Commissioner cooperates in these proceedings as the authority concerned. These procedures are aimed at supervising the compliance of these controllers with the GDPR, both in terms of the lawfulness of personal data processing as well as the adequacy of their privacy policies and the information given to the individuals about the processing, the exercise of their rights, and violations of personal data protection due to breaches into information systems and the lack of appropriate security measures.

Cooperation in cross-border inspection cases, as introduced by the GDPR, is undoubtedly one of its key novelties and strengths, notably in terms of the uniform functioning of the supervisory authorities in the various EU and EEA Member States. A uniform approach is the only way the EU supervisory authorities can influence the activities of multinational internet service providers, communication platforms and social networks, whose business model is most often based on a service that is free to the user but monetized through personalized and targeted advertising based on processing vast quantity of personal data. These services are used by individuals throughout EU and EEA Member States, and supervisory authorities now have robust mechanisms and close cooperation tools in place to address in unified manner controversial practices that are detrimental to the rights of individuals. It should be noted that such cooperation poses a great challenge for the Information Commissioner and other supervisory authorities in terms of the need for additional resources, both financial and human resources. A specific knowledge is needed to deal with such cases and should involve different disciplines, from law, information technology, economics, modern advertising industry and social media. Excellent knowledge of the English language is key, as English is the operational language in cross-border procedures mentioned. Finally, administrating such cooperation through a new information platform, which institutionalized the procedures, also requires additional resources.

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 Commissioner engages in international cooperation and in the legislative procedures of the EU as envisaged by the 95/46/EC Directive. Thus, in 2018, the Information Commissioner participated at the EU level at plenary meetings and in the work of several subgroups of the Working Party established under Article 29 of the 95/46/EC Directive (The Article 29 Data Protection Working Party - WP29). In 2018, the Working Party 29 focused primarily on the upcoming coming into force of the GDPR and the establishment of the European Data Protection Board (EDPB), an independent European body for ensuring a consistent application of the data protection rules in the EU and for encouraging cooperation between EU data protection authorities. It was established in May 2018 in accordance with the GDPR and has a seat in Brussels. It follows its own Rules of Procedure 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 2018, 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 2018 in the International Working Group on Data Protection in Telecommunications (IWGDPT), bringing together the representatives of information commissioners and data protection and privacy authorities from all over the world.

INITIATIVE 20i7
In 2017, the Information Commissioner initiated the "**Initiative 20i7**" in order for data protection supervisory authorities from the former Yugoslavia to join forces, as they face similar professional issues and challenges. As many companies and public sector organizations in the region collect and exchange personal data cross-border, it is vital to ensure appropriate and uniform level of personal data protection also from an economic perspective. The objective of Initiative 20i7 is to foster close cooperation and exchange good practices in the area of personal data protection in the region. Such an initiative in the field of human rights protection can further contribute to strengthening good relations between the countries involved.

At the second meeting of Initiative 20i7, in Macedonia in April 2018, the heads of data protection supervisory authorities from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia and Slovenia discussed the challenges that arise at the national levels when implementing the new European standards for the protection of personal data.