NEJVYŠŠÍ SPRAVNI SOUD

Seminar organized by Supreme Administrative Court of the Czech Republic and ACA-Europe

Supreme administrative courts and evolution of the right to publicity, privacy and information.

Brno, 18 May 2015

Answers to Questionnaire: Slovenia

Seminar co-funded by the "Justice" programme of the European Union

Supreme Administrative Courts and evolution of the right to publicity, privacy and information

Republic of Slovenia

(Answers to questionnaire)

1 Briefly describe the administrative institutional backing of free access to information and of the protection of personal data. Whenever those agendas are institutionally linked, provide for a brief description of such relations.

In the Republic of Slovenia, the Information Commissioner is an autonomous and independent administrative authority, competent of supervising both: access to public information and the protection of personal data.

The Information Commissioner was established on 31 December 2005 by the *Information Commissioner Act* (Slovenian: ZinfP) which merged the Commissioner for Access to Public Information with the Inspectorate for Personal Data Protection and the Information Commissioner, as we know it today, was established, with combined competences.

Access to public information

In the field of access to public information, the Information Commissioner has according to the *Access to Public Information Act* (Slovenian: ZDIJZ) the role of an appellate authority competent to decide on appeals against an authority's decision to deny or refuse an applicant's request or in any other manner violate the right to access or re-use of public information, and also, with regard to appellate proceedings, to supervise the implementation of the law regulating access to public information and the regulations adopted thereunder.

In the field of access to public information, the Information Commissioner also has competences as determined by the *Media Act* (Slovenian: ZMed). According to the Media Act, a responsible authority's negative response to a question posed by a representative of the media shall be considered as a rejection of the request. The non-responsiveness of a responsible authority in such an instance is an offence, as well as grounds for a complaint. The Information Commissioner makes a decision with regard to a complaint against a rejected decision, pursuant to the provisions of the *Access to Public Information Act*.

Protection of personal data

In the field of personal data protection, the Information Commissioner has under the *Personal Data Protection Act* (Slovenian: ZVOP-1) among others jurisdiction to:

1. carry out inspections regarding the implementation of *Personal Data Protection Act* and other regulations governing the protection or processing of personal data (consideration of complaints, appeals, messages and other applications referring to suspected violations of the

law, and carrying out planned preventative inspections of data controllers in the public and private sector),

2. decide in relation to complaints made by individuals when the data controller denies the request of the individual regarding their right of familiarisation with the requested data, printouts, lists, access, certificates, information, clarifications, transcriptions or copying in accordance with provisions of the law that regulate the protection of personal data,

3. conduct minor offence proceedings in the area of personal data protection,

4. publish, on the website and in any other appropriate manner, preliminary opinions on the compliance of draft laws and other regulations, with the law and other regulations pertaining to the protection of personal data, and requests for constitutional reviews of regulations, publish court decisions relating to personal data protection and non-binding opinions, interpretations, observations and recommendations concerning personal data protection in individual areas.

According to the *Personal Data Protection Act* the protection of personal data is also a specific area of the Ombudsman, of which the Deputy Ombudsman is in charge. His role is, however, only advisory.

The Slovenian *Criminal Code* (Slovenian: KZ-1) in Article 143 provides additional protection of individuals from abuse of their personal data.[1] It defines the merits of a criminal offence consisting in an unlawful use of personal data. This provision enables criminal prosecution of the most serious cases of unauthorized use of personal data.

Other competences of the Information Commissioner

The Information Commissioner also functions as a minor offence authority, responsible for the supervision of the implementation of *Access to Public Information Act* and *Personal Data Protection Act.*

The Information Commissioner can also 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.

1 (1) Whoever unlawfully uses personal data, which may be kept only on the basis of the law or on the basis of the personal consent of the individual, to whom the personal data relate, shall be punished by a fine or sentence to imprisonment for not more than one year.
(2) Whoever breaks into a computer database in order to acquire personal data for his or a third person's use shall be punished in accordance with the preceding paragraph.
(3) Whoever publishes on the World Wide Web or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the law or court decision, on the basis of which these persons may be identified or are identifiable, shall be sentenced to imprisonment for not more than three years.
(4) Whoever assumes the identity of another person and under its name exploits their rights, gains property benefits or damages their personal dignity shall be sentenced to imprisonment between three months and three years.
(5) If any offence from the preceding paragraphs of this Article is committed by an official through the abuse of office or official authority, such an official shall be sentenced to imprisonment for not more than five years.

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 an independent supervisory body responsible for supervising the transfer of personal data for the purposes of the Convention.

2 Describe in general terms the regular administrative and court procedure in a typical disputable case of free access to information. Describe also the procedural role of your supreme administrative instance.

The request for public information may be informal (oral) or formal (in writing). However, only the applicant who files a written request enjoys legal protection from unjustified refusal of his/her request. The applicant files a request for the information with the body which supposedly holds the information the applicant wishes to gain access to. In his request, the applicant has to specify: the information he wishes to gain access, the way he wishes to access the requested information (consultation on the spot, a transcript, a copy, an electronic record). The applicant is not required to give the legal grounds for the request or expressly characterize it as a request for the access to public information.

If the public body, which has received the request, does not hold the information, it must immediately, within the time limit of 3 working days, assign the request to the body which is competent for resolving the request and notify the applicant. On the other hand, if the public body would otherwise be competent for the applicant's request but does not hold the requested information, it must issue a decision, denying access to the public information on the ground that the information does not exist (the public body does not hold the information).

Administrative silence

When the public body does not respond to the applicant's request or does not provide the public information in due time (within 20 working days from receiving the request), the applicant can appeal to the Information Commissioner.

Upon receiving the appeal, the Information Commissioner must inquire with the body as to why there was no response. Should it recognize that the reasons for delay were justified, it prolongs the deadline for the body to decide on the applicant's request (but for no longer than 30 days). However, if the reasons for delay are not justified (according to the assessment of the Information Commissioner), the Information Commissioner decides to take one of the following steps. One possibility is to take over the case and issue a decision instead of the public body. The second, more frequent option is to demand from the public body to issue a decision within a certain time limit, if this were more economical and faster than to take over the case. Should the public body (even after receiving a written call to issue a decision) fail to do so, the Information Commissioner issues the decision itself.

Refusal by decision

When the public body refuses the applicant's request in whole or in part, the applicant can file the appeal with the body. If the applicant first appeals directly to the Information

Commissioner, the Information Commissioner has to immediately send the appeal to the public body.

Upon receiving the appeal, the public body must first check all the procedural requirements – whether the appeal is allowed, whether the appellant has the right to appeal and whether the appeal was filed within the prescribed time limit (15 days after the decision). If any of these procedural requirements are not fulfilled, the body dismisses the appeal by an order. The applicant may appeal against this order.

If the procedural requirements are fulfilled, the body sends the appeal to any of the entities whose interests might be affected by the appellate procedure (e.g. the requested information represents their business secret), invite them to participate in the procedure and provide any relevant information or their position on the matter.

The public body has the possibility to decide upon the appeal itself by amending its first decision. The applicant can also appeal against this new, amended decision.

If the public body finds that the procedural requirements are fulfilled and insists on its first decision, it sends the appeal, together with all the relevant documentation to the Information Commissioner. The body has 15 days to check all the procedural requirements and send the appeal to the Information Commissioner. If the body fails to send the appeal, the applicant (or the Information Commissioner) can report the body to the Public Administration Inspectorate.

Decision on an appeal

Upon receiving the appeal and the documentation, the Information Commissioner also checks the procedural requirements. If those are not fulfilled, the IC dismisses the appeal by order. Otherwise, the IC decides on the subject matter. The Information Commissioner can:

- refuse the appeal in whole or partially as unfounded and confirm the public body's decision;
- grant the appeal in whole or partially, overthrow the body's decision and order the body to hand out the requested public information or part of it for re-use;
- grant the appeal in whole or partially, overthrow the body's decision and refer the matter back to the body to issue another decision within 30 days;
- annul the body's decision.

The Information Commissioner has to issue a decision immediately and at the latest within 2 months from receiving the complete appeal.

The Information Commissioner's decision is binding (not abiding by it constitutes a misdemeanour). However, any of the parties involved may begin an administrative dispute against the Information Commissioner's decision before the Administrative Court.

Administrative dispute

Administrative dispute refers to judicial protection of one's rights and legal interests against decisions and actions of administrative authorities and bearers of public authority, which includes also the Information Commissioner. It is prescribed in the *Administrative Dispute Act* (Slovenian: ZUS-1).

Administrative dispute encompasses two levels of judicial protection: the Administrative Court on the first instance and the (administrative department) of the Supreme Court on the second instance. Administrative Court decides on actions against acts, herein Information Commissioner's decisions, while the Supreme Court decides on appeals and revisions against acts adopted by the Administrative Court.

Administrative Court

An applicant can file an action against Information Commissioner's decisions for a judicial control of the procedural law, substantive law and the correct finding of the state of facts.

Administrative Court has to decide a case according to the claims, posed by the parties and within the limits of the reasons invoked by them. Under these terms the court examines the relevant substantive rules *ex offo*.

Generally, the control of the Administrative Court is limited to assessment of illegality of contested acts. Only exceptionally may the court also remove the administrative act and decide on the matter by issuing a decision instead of the administrative body (dispute of full jurisdiction).

Supreme Court

Decision taken by the Administrative Court can be challenged by an appeal (ordinary judicial remedy) or a revision (extraordinary judicial review). Both are decided on by the Supreme Court. They are mutually exclusive.

An **appeal** is allowed only if Administrative Court has ascertained facts differently than the administrative authorities and has on the basis of these new facts changed the administrative act. An appeal is exceptionally allowed also if Administrative Court decides on an applicant's action in which the applicant stated that his constitutional rights were infringed.

On the other hand, a **revision** is allowed only:

- if the value of the contested part of the final administrative act or final ruling, when the court took substantive decision, in the matters where the right or obligation of a party is expressed in monetary value, exceeds EUR 20.000;

- if the substance of the matter concerns the decision on a relevant legal issue or if the ruling of the court of first instance deviates from the case law of the Supreme Court with regard to the legal issue that is essential for the decision, or if there is no uniform position concerning this legal issue in the case law of the court of first instance and the Supreme Court has not yet adjudicated on the matter;

- or if the decision that is being contested in the administrative dispute has very grave consequences for the applicant.

A revision may be filed due to essential violations of the provisions on the procedure and due to erroneous application of substantive law. It can not be filed due to incorrectly or incompletely established state of facts. The court examines the relevant substantive law *ex offo*.

Constitutional Court

In the Republic of Slovenia, the right to the access to public information (as well as the right to personal data protection) is a constitutional right (Article 38 and 39 of the *Constitution of the Republic of Slovenia*, Slovenian: Ustava Republike Slovenije). Therefore, in case of a violation of this right, e.g. with the Supreme Court's decision, an applicant has another legal remedy - constitutional complaint.

3 Describe the procedural role of your supreme administrative instance in the agenda of protection of personal data.

Every individual is entitled to file an complaint to the Information Commissioner if he believes that a person (either public or private) is infringing the *Personal Data Protection Act*. The Information Commissioner can according to his official duties start all appropriate inspection proceedings.

The Information Commissioner who in performing inspection detects a violation of *Personal Data Protection Act* or of another statute or regulation regulating protection of personal data has the right:

1. to order the elimination of irregularities or deficiencies he detects in the manner and within the interval he himself defines;

2. to order the prohibition of processing of personal data by persons in the public or private sector who have failed to ensure or failed to implement measures and procedures to secure personal data;

3. to order the prohibition of processing of personal data and the anonymising, blocking, erasure or destruction of personal data whenever he concludes that the personal data are being processed in contravention of the statutory provisions;

4. to order the prohibition of the transfer of personal data to third countries, or their supply to foreign data recipients, if they are transferred or supplied in contravention of the statutory provisions or binding international treaty;

5. to order other measures provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure.

The Information Commissioner is obliged to notify complainant of all important conclusions and actions in the procedure of inspection. There is no appeal against a decision or ruling of the Information Commissioner, but an administrative dispute is permitted (for explanation of further procedure see the answer under the question 2).

The personal data controller must on an individual's request:

- enable the examination of the personal database's catalogue;

- confirm whether the data in connection with an individual is or is not being processed, and enable the individual examination thereof, as well as its transcription or copying;

- transmit a copy of personal data, contained in the personal database, referring to the individual;

- transmit a list of users, the data was transmitted to, when, on which legal grounds and for what purpose;

- give information on sources, on which the database entries referring to an individual are based, and on the method of processing;

- give information on purpose of processing and type of personal data being processed, as well as all necessary pertaining explanations;

- explain technical or logically-technical decision procedures in case automated decision-making of an individual's data is being performed.

The Information Commissioner is competent for deciding on the appeal of an individual when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy.

Judicial control against the decision of the Information Commissioner in provided. Applicants have the possibility to initiate an administrative dispute and file constitutional complaint (for additional information of the procedure see the answer under the question 2).

4 Provide for a general overview of historical development of access to information rights in your jurisdiction while focusing on most important legislative and judicial milestones. Also, please try to generally describe the main driving forces behind the development of these rights.

The right to access public information was granted by the legislature already in the *Constitution of the Republic of Slovenia*[2]. 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*[3], which ensures everyone free access to and re-use of public information held by state bodies, local government bodies, public agencies, public funds, and other entities under public law, bearers of public authority, and public service contractors.

The mentioned Act actually broadens the constitutional right as it does not demand from an applicant to have a well-founded legal interest under law in order to gain an information of a public nature. An information is either public or not and if it is public, it is irrelevant why would someone want to have it or how to use it. Therefore, some legal experts call for change of the Constitution in order for this right to be refined, broadly interpreted and protected.[4]

The most important milestones in the field of transparency[5]

2 Official Gazette No. 33/1991, dated 28 December 1991.

3 Official Gazette No. 24/2003, dated 7 March 2003.

4 U. Prepeluh Magajne in: L. Šturm, Ed., Komentar Ustave Republike Slovenije: dopolnitev komentarja – A (Commentary on the Constitution of the Republic of Slovenia: Supplement to the Commentary – A), Fakulteta za podiplomske državne in evropske študije (Faculty of Postgraduate National and European Studies), Ljubljana, 2011, p. 589-590.

5 Partly adopted from Information Commissioner's Annual report 2013, available on the page: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual_Report_2013.pdf (12 March 2015).

1. Increased transparency in the use of public funds – Partly as a result of decisions by the Information Commissioner (e.g. decision, wherein a member of the media requested, from the office of the former President of the Republic of Slovenia, a list of names of guests that had attended a dinner hosted by the then President, at Villa Podrožnik), the *Access to Public Information Act* was amended in 2005 with the provisions, which provides that information regarding the use of public funds, regardless of possible exemptions, is always to be publicly available.

2. Increased transparency in public procurement procedures – Also as a result of practices of the Information Commissioner (e.g. decision, wherein the applicants, otherwise potential suppliers in particular public tenders, requested access to information of offers submitted in public procurement procedures of various ministries), in 2010 the provisions of the *Public Procurement Act* were amended to explicitly provide that: quantity specification, price per unit, value of individual items and total value of an offer are public information, and in cases where the most economical offer is sought, other data which influenced the ranking of offers, based on the application of additional criteria.

3. The introduction of the public interest test following amendments to the *Access to Public Information Act* in 2005 – Prior to the first change of the Act, the Information Commissioner repeatedly emphasised the importance of balancing the various human rights in procedures regarding requests for access to public information. The public interest test or balance test was for example carried out in 2004, in a case, wherein a journalist requested details of the salaries of executive employees at RTV Slovenia.

4. Public sector salary disclosure – Partly as a result of a decision by the Information Commissioner in a matter regarding a journalist's request for details of salaries of former public servants, there were changes made to the *Public Sector Salary System Act* (Slovenian: ZSPJS) in 2005. Provisions were added to this Act, which explicitly provide that, in accordance with procedures regulated by the *Access to Public Information Act*, the individual details of gross wages of every public servant and every public official, before deductions for attachment of earnings, loan repayments or other personal obligations, are to be publicly available.

5. Public disclosure of Notary income procurement – In 2004, the Information Commissioner dealt with a journalist's request, addressed to a number of Notaries, for information to be forwarded from annual financial statements, of the income and profit derived from carrying out the notary work. The Information Commissioner was of the opinion that such information was freely accessible public information. In proceedings before the Supreme Court, the Information Commissioner's argument was dismissed by judgement No. I Up 122/2006, dated 25 April 2007. Therein, the Supreme Court stated that "when defining certain information as public information it is essential for that information to reflect the fact or circumstance that affects or could affect the exercise of public functions. Otherwise (when it comes to activities of the body on the free market) we can not speak about public information that originates from the field of work of an authority and therefore there is no public information within the meaning of *Access to Public Information Act"*.

6. Greater transparency in the recruitment of public servants and their contracts of employment. – In a number of matters the Information Commissioner, using a broad interpretation, which is in the interests of transparency, established good practice for public access to documents relating to the employment contracts of public servants (e.g. documents which indicate if the public servant meets the requirements to fill a given position).

7. Greater transparency of the activities of legal persons governed by public law sui generis – In a number of matters the Information Commissioner drew attention to the non-transparent activities of legal persons governed by public law sui generis and was of the opinion, that these organisations were also covered by *Access to Public Information Act*. On a number of occasions the Supreme Court confirmed that such a view was valid, and the decisions handed down in these cases contributed to more transparent activities of these responsible entities in practice.

In judgement No. X Ips 638/2008, dated 20 May 2009, the Supreme Court stated that "the *Access to Public Information Act* does not specify the criteria on the basis of which it would be possible to identify the applicant as a legal person governed by public law. It is therefore necessary to use the legal theory. According to legal theory, the fundamental elements of the legal regime relevant to the identification of legal persons governed by public law are: the act of establishment, the nature of the functions and activities, resources and funding, and the use of the public or private law in the internal and external relationships". In judgement No. X Ips 318/2010, dated 6 July 2011, the Supreme Court adjudged that "Student Organization of the University is a legal person under public law within the meaning of the *Access to Public Information Act* and is therefore liable for providing public information".

8. The amended *Access to Public Information Act* (2014), which has extended the circle of responsible authorities to include business entities, which are primarily controlled by the state, local authorities and other legal entities governed by public law.

9. Adoption of the Council of Europe *Convention on Access to Official Documents* (Slovenia was among the first 12 signatories) – Slovenia together with Information Commissioner Nataša Pirc Musar, as expert advisor for the Council of Europe, played an important role in the drafting of the Convention, which sets minimum standards with respect to the individual's right of access to official documents. Following successful ratification by the Council of Europe Member States, this right will become internationally recognised as a fundamental human right. However, Slovenia has not yet ratified the Convention.

10. In recent case No. U-I-201/14, U-I-202/14, dated 19 February 2015, the Constitutional Court ruled on the constitutionality of *Access to Public Information Act* as regards the publicity of information held by the banks that have benefited from the public stabilization measures. The Constitutional Court decided that information directly related to the individuals' loans, which have not been transferred to the *Bank Assets Management Company* (Slovenian: Družba za upravljanje terjatev bank) should not be public. Otherwise, another constitutional right to free economic initiative would be disproportionately affected.

The main driving forces behind the development of these rights were in the first place the media, that initiated many of the administrative proceedings that led to the aforementioned

decisions and to disclosure of important public sector information, but also a strong inclination of some politicians (e.g. Minister for information society when *Access to Public Information Act* was adopted in 2003, Minister for internal affairs when *Access to Public Information Act* was amended in 2014) towards transparency of public sector, and a very active role of Information Commissioner through all the years since its establishment.

5 Give basic subjective observation as to the role and importance of free access to information in political system of your country. In particular, focus on how the importance of freedom of information is perceived by general public and by non-governmental sector.

The Supreme Court has no official information on the subject therefore it can not provide any information apart from the information gathered and published by the Information Commissioner in his Annual report for the year 2013 (see below).[6]

The volume of work dealt with by the Information Commissioner has grown rapidly since the autumn of 2003. In 2006 the Commissioner received 504 complaints and issued 101 decisions related to access to public information issues, 231 reports of violation of personal data protection were received and 180 inspection procedures were carried out. By the year 2010, the number of complaints, related to requests for access to public information had risen to 610 (258 decisions were issued), similarly the number of reports related to the violation of personal data protection also increased, necessitating 712 inspection procedures.

The response from individuals confirms that the Commissioner's work has been effective. As early as 2008 the Politbarometer poll, covering public opinion research on the level of trust people have in public institutions, and with the Information Commissioner included for the first time, showed that 47 % of people polled rated the Commissioner as trustworthy, ranking it fourth behind the President of the Republic of Slovenia (55 %), the Euro (53 %) and the Bank of Slovenia (49 %). The Commissioner was also placed high on the list of the same survey carried out in later years. In January 2013, people surveyed rated the Information Commissioner at the very top of the list of authoritative figures of state supervisory bodies, followed, in equal second place, by the Ombudsman and the President of the Court of Auditors.

Results of the work of the Information Commissioner are evident also in the general public's high level of awareness. At the end of April 2008, the European Union published the results of the Eurobarometer public opinion survey which looked at the awareness, attitudes and views of citizens of each of the 27 member states with regard to personal data protection as well as their perception of personal data controllers. The poll showed that, as far as understanding the problems, in most of the areas covered in the survey Slovenia ranked at the top of the EU. In the field of access to public information, protection of the right of access to public information was shown to be at a high level as indicated in the research published in 2013 by the International organisations Access Info Europe (Spain) and Centre for Law and Democracy (Canada), which out of 89 countries, placed Slovenia in an impressive second

6 Adopted from Information Commissioner's Annual report 2013, available on the page: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual_Report_2013.pdf (12 March 2015).

position with regard to the area of legislative regulation covering access to public information. The increase in the number of complaints in this area shows that individuals are also becoming more aware of their rights.

6 Give subjective general observation as to whether and eventually how free access to information rights are in practice abused or misused by the petitioners.

As it can be seen from the Administrative Court case-law (e.g. judgement No. III U 240/2012, dated 7 November 2013) abuses and misuses do occur in practise.

In the mentioned case an administrative authority, obliged to give public information, received in 2011 a total of 202 requests for public information, of which 51 requests were from the plaintiff in the subject matter. In 2012, it received 86 requests, of which 66 requests were from the plaintiff. In addition, in 2012 the authority received 322 e-mails from the plaintiff. In these requests, the plaintiff required an access to a very large number of documents, for example: the entire correspondence between two public authorities, one private company, the Commission for Prevention of Corruption, the Ombudsman, the police, public prosecutors, the relevant ministries etc. The Administrative Court (the same as the administrative authority and the Information Commissioner) held that the plaintiff by sending such a large number of requests for access to public information actually abused his right. Namely, his purpose was not only access to information in the name of exercising democratic and supervisory function of the right of access to public information, but he also with his way of filing requests disproportionately burdened the authority, what constitutes an obstacle to its effective work not only in the field of access to public information, but in all its areas of work.

The abuses and misuses of *Access to Public Information Act* that occasionally occurred in practice eventually led to the adoption of new provision in the 2014 amended *Access to Public Information Act*, which now states in Article 5 that the body may exceptionally deny the applicant access to requested information in the event the applicant with one or more functionally connected requests manifestly misuses its right to access public information under this Act or it is clear the request or requests are of vexatious character.

7 Give a list and brief explanation of security, law enforcement and/or defence institutions that can benefit in your country from the exceptions laid down in Art. 7(e), Art. 8(4) and 8(5) of the Directive 95/46/EC.

The *Personal Data Protection Act* in Article 36 stipulates: “The rights of an individual from (the third and fourth paragraphs of Article 19, Articles 30 and 32 of) this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the

police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

Restrictions from the previous paragraph may only be provided in the extent necessary to achieve the purpose for which the restriction was provided.".

This provision is specific because it provides for sectoral legislation to restrict some rights of individuals guaranteed under the *Personal Data Protection Act*. However, the principle of proportionality must nevertheless be respected.

There is no officially confirmed list of institutions that can benefit from the exceptions laid down in the mentioned Directive. The sectoral legislation determines such institutions for each relevant sector. For example: the police under the *Police Act*, Ministry for Foreign Affairs under the *Restrictive Measures Act*[7], Slovene Intelligence and Security Agency under the *Slovene Intelligence and Security Agency Act*, Intelligence and Security Service (under the Ministry for Defence) under the *Defence Act*, tax authorities under the *Tax Procedure Act* etc.

8 Subjectively identify most emerging actual problems that arise from processing of personal data by aforementioned security, law enforcement and/or defense institutions. Whenever appropriate, demonstrate them on particular examples.

The Supreme Court has not yet encountered problems on such issue.

However, as seen from the Constitutional Court case-law (judgement No. U-I-312/11, dated 13 February 2014) there have been questions regarding the constitutionality of the *Police Act* in that matter. In the mentioned case the Constitutional Court held the following:

„DNA profile is personal data and its processing presents an interference with the privacy of the individual, protected by the first paragraph of Article 38 of the Constitution.

However, processing and thus storage of DNA profiles follows a permissible goal of detecting criminals due to the effective protection from criminal activity.

Regulation in the *Police Act*, which allowed the police for the purpose of detection of the offender or in order to establish his identity in its current collection to keep the DNA profile of an individual who was suspected of having committed an offence, but was not finally convicted, all the way to the limitation period for prosecution, was not necessary to achieve the objective of the legislature. It has therefore inadmissible interfered with the right of the first paragraph of Article 38 of the Constitution. In the light of the purpose of storage, the legislature could substantially the same effects or effects which are essentially comparable to

7 Restrictive measures and/or sanctions are measures by which the international community tries to achieve that certain states and/or other entities (persons) presenting a threat to international peace and security change their conduct without the use of force, so that this does not threaten international peace and security.

limitation period for prosecution reach already by limiting to other decisions that have a res iudicata effect, which do not constitute a final conviction of the perpetrator but they mean an end of criminal proceedings and that the prosecution against an individual in this case is no longer admissible.

Regulation in the Police Act, which allowed that the DNA profile of an individual who was suspected of having committed an offence but was not convicted, is permanently stored, was not necessary to obtain a constitutionally permissible goal. Access to the data was not significantly circumscribed, therefore, there was not any circumstance that would allow an assessment of whether the permanent storage of DNA profiles of those persons meets the requirements for interference with the privacy of an individual."

In another case (wherein the Constitutional Court issued decision No. U-I-45/08, dated 8 January 2009) an issue of lawfulness of invasions of privacy and personal data protection conducted by the Slovene Intelligence and Security Agency occurred.

In the mentioned case the Information Commissioner filed a request for a constitutional review of the *Slovene Intelligence and Security Agency Act* (Slovenian: ZSOVA) and alerted to the provisions of Article 21, on the basis of which a database of personal data was being created in connection with the strategic monitoring of telecommunications and which was, in the Information Commissioner's opinion, unconstitutional. The Constitutional Court dismissed the request on procedural grounds and made no decision on its merits. For that reason there is no judicial position on the constitutionality of the regulation.

Date: 23 March 2015