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: Lithuania

Seminar co-funded by the “Justice” programme of the European Union

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

Lithuania

(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.

Free access to information

There is no administrative authority responsible specifically for free access to information in Lithuania. However, the complaints of this kind may be addressed to an administrative disputes commission (regional or central) which carries out pre-trial investigation of administrative disputes including those related to free access to information. Applicant may also address their complaints to the Ombudsman ('Seimo kontrolierius') whose function is to investigate complaints about abuse of power, bureaucracy and other kinds of human rights violations in public administration. Submitting complaint to the Ombudsman or to an administrative disputes commission is by no means compulsory procedures before starting court proceedings. Thus in case the requested information is not provided, the person concerned may straightaway start court proceedings in administrative court.

Protection of personal data

The National data protection inspection (hereinafter – NDPI) is an administrative institution responsible for the supervision of data controllers' activities. Basically, it is ensuring the protection of data subject rights. The NDPI examines complaints, reviews lawfulness of data processing and makes decisions with regard to data processing infringements. It also provides guidance for data subjects, data controllers and processors, other persons with regard to protection of personal data and privacy, publishes general guidelines about personal data protection. Applying to the NDPI is not compulsory before applying to court, however, it might be less costly and less time-consuming for the applicant if the dispute is settled in the NDPI and no further recourse to court is needed.

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.

Everyone willing to access certain information must submit an application to the institution which is in control of the information in question. The information must be delivered to the applicant within 20 working days following the day when the application was received by the institution. If the information in question is voluminous or complicated, the head of the

institution has the right to extend this term for another 20 working days and notify the applicant about the decision taken, stating reasons thereof. In case the institution refuses to provide the requested information, it notifies the applicant, specifying the reasons thereof and the appeal procedure. The decision of the institution (to provide certain information or not to provide any) may be appealed against before administrative court not later than within one month following the delivery of the decision to the applicant or within two months following the last day when the decision had to be taken, but was not taken. The decision of the administrative court of first instance may be appealed to the Supreme Administrative Court of Lithuania (hereinafter – SACL) within 14 days following its delivery. The SACL decides on questions of both law and fact and its decisions are not subject to appeal.

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

The NDPI, after investigating the complaint, has the right to: 1) declare the complaint to be well-founded; 2) reject the complaint; 3) terminate investigation of the complaint. A person that has suffered harm due to the unlawful processing of personal data has also the right to claim pecuniary and non-pecuniary damage. The damages are assessed by the court. Decisions of the NDPI may be appealed against before the administrative court of first instance within one month following their delivery. As mentioned above, the decision of the administrative court of first instance may be appealed to the SACL within 14 days following its delivery. The SACL decides on the questions of both law and fact and its decisions are final and not subject to appeal. Having heard the case the SACL has the right to: 1) reject the appeal and uphold the decision of the court of first instance; 2) annul the decision of the court of first instance and take a new decision; 3) change the decision of the court of first instance; 4) annul the decision of the court of first instance and remit the case in whole or in part to the court of first instance; 5) annul the decision of the court of first instance and terminate the proceedings or leave the claim unexamined.

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 Constitution of the Republic of Lithuania adopted in the Referendum of 25 October 1992 (Art. 25) states:

The human being shall have the right to have his own convictions and freely express them.
The human being must not be hindered from seeking, receiving and imparting information and ideas.
Freedom to express convictions, to receive and impart information may not be limited otherwise than by law, if this is necessary to protect the health, honour and dignity, private life, and morals of a human being, or to defend the constitutional order.
Freedom to express convictions and to impart information shall be incompatible with criminal actions—incitement of national, racial, religious, or social hatred, violence and discrimination, with slander and disinformation.
The citizen shall have the right to receive, according to the procedure established by law, any information concerning him that is held by State institutions.

According to the case-law of the SACL, the right to receive information from the state institutions is granted a constitutional protection under Art. 25 of the Constitution. This right is further regulated by the Law on the Right to Access Information from State and Municipal Institutions (hereinafter – the Law on the Right to Access Information) which was enacted in 2000. This law regulates the conditions and procedures for the implementation of the aforementioned right, the principles of the provision of information, the exceptions when information is not provided and the cases when an institution may lawfully refuse to provide information. In 2005 this Law was amended in order to implement the Directive 2003/98/EC of the European Parliament and of the Council on the re-use of public sector information. Another relevant law in the sphere is the Law on the Provision of the Information to the Public which establishes the procedure for collecting, producing, publishing and disseminating public information and the rights, duties and liability of producers and disseminators of public information, their participants, journalists and institutions regulating their activities.

Several developments with regard to the right to access information could be pointed out. One should note the legal developments concerning the definition of the term 'public institutions'. It was amended in 2008 when the Law on the Right to Access Information was changed in order to disclose information about the salaries of employees of a wider circle of state and municipal institutions.[1] Initially the term 'State and municipal institutions' was defined as representative, head of state, executive institutions and judicial authorities, law enforcement agencies and institutions exercising control (supervision) and other state and municipal institutions and bodies, which are financed by state or municipal budgets and state funds and which are conferred administrative powers by the law, as well as enterprises and institutions providing public services. In 2008 this definition was further elaborated, adding that the 'state and municipal institutions' were also 'state and municipal companies, public enterprises the owner or one of the owners of which is the state or a municipality, joint-stock companies and limited liability companies in which the state or a municipality holds more than 50 percent of votes at the general meeting of shareholders, when they provide information about their employees' salaries under this law.' Few years later these legal provisions regulating the right to access information about salaries of public institutions employees were interpreted in a case before the Supreme Administrative Court of Lithuania[2]. Applicant in this case claimed that he has the right to be provided information about salaries of several public hospital employees. The SACL decided that legal provisions of the Law on the Right to Access Information conferred the right to access general information about the salaries paid to certain types of positions at the hospital but did not entitle everyone to access particular salaries of concrete employees. The SACL stated in this case that the public interest does not justify the need to access information about salaries of particular employees.

One should also note that the NGO's in Lithuania are fairly active in the field of access to information. E. g., the Human Rights Monitoring Institute has lodged a complaint before administrative courts in 2013 demanding to declassify a certain document possessed by the State Security department, arguing that the document contained information of public interest and possibly about illegal acts of state officials and human rights violations. The same NGO has

[1] http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=319057
[2] Case No. A[492]-2809/2011 (22 September 2011).

carried out a study[3] about the right to access information in Lithuania wherein it called among other things for establishing procedures that would allow lodging requests to declassify information in cases when the information is of public interest or when it was classified without a good reason.

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.

Free access to information is an inherent part of democracy in Lithuania as well as in other countries. Having access to information facilitates the freedom of expression, allows criticism and encourages development. It appears that in Lithuania the citizens are not particularly active in defending their right to access information as there have been only few significant cases in the administrative jurisdiction. The reason could also lay in sufficiently clear law that is applied without court intervention in practice. However, the NGO's are becoming more active in voicing the deficiencies in implementation of the above-mentioned right.

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.

In most of the cases heard by administrative courts the applicants claim the right to information with regard to the pre-trial investigation material. However, this does not appear to be misuse but rather incomprehension of the right to access information. Therefore, it does not appear that this right is abused by petitioners.

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 Law on the Legal Protection of Personal Data does not enlist security, law enforcement or defence institutions that can benefit from the exceptions laid down in Art. 7(e), Art. 8(4) and 8(5) of the Directive 95/46/EC. Art. 1(6) of the Law states that in processing personal data for the purposes of state security and defence, this law applies to the extent that other laws do not specify otherwise. There are several other laws which provide for specific regulation in this regard. E. g., the Law on Corruption of Prevention confers the right to the Special Investigation Service to collect information about past convictions, allegations of corruption, administrative offences, etc. This information is collected before employing a person and provided to the employer in order to estimate the prospective employee's reliability and reduce the risk of corruption in state institutions. The Law on Special Investigation Service states that state and municipal institutions and enterprises must allow the Special Investigation Service to use state registers, cadastres and other data banks free of charge, other companies and organizations must allow using their data banks according to contracts.

[3] https://www.hrmi.lt/uploaded/Documents/Teise_gauti_informacija_ZTSI_2014.pdf

According to the Law on Secret Intelligence ('Kriminalinės žvalgybos įstatymas'), the main secret intelligence institutions are the Financial Crimes Investigation Service, the Prison Department under the Ministry of Justice, the Customs Department under the Ministry of Finances, the Police Department under the Ministry of the Interior, the Secret Investigation Service, VIP Protection Department under the Ministry of the Interior, the State Border Security Department under the Ministry of the Interior. Subdivisions of the aforementioned institutions that are authorized to carry out secret intelligence service have the right inter alia to receive data from the main state information registers, information systems and data bases and to secretly obtain finger prints, voice, smell and other samples for investigation. Secret intelligence institutions may also perform the following actions provided court permission is granted: 1) obtain information about electronic communications networks and traffic data users from operators of electronic communications networks and (or) services; 2) obtain information about economic, financial transactions, the use of financial and (or) payment means from the Bank of Lithuania, finance companies and credit institutions, as well as other legal entities; 3) obtain other information possessed by legal persons when court permission is needed to obtain the particular type of information; 4) secretly inspect, control, confiscate mail and other communications; 5) secretly enter, inspect private residences, employment and other premises, closed areas, vehicles, take documents, samples of substances, other objects needed for secret intelligence and mark them; 6) simulate criminal conduct (state prosecutor's permission is required); 7) carry out secret surveillance (state prosecutor's permission is required when it is carried out for longer than 3 days).

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

Lithuanian legal jurisprudence points out the lack of clarity of legal provisions and inaccessibility of certain legal provisions regulating secret intelligence as main problems in this sphere.[4]

The Supreme Administrative Court of Lithuania has also faced the issue of lose regulation of secret intelligence institutions powers in a case where wiretapped conversations were used to prove that a disciplinary offence was committed. In that case[5] the SACL has noted that secret intelligence acts affect the essence of human rights and the legal provisions that limit human rights may not be interpreted and applied broadly. The court stated that laws did not stipulate that secret intelligence may be used to prove disciplinary offences and interpretation of the Criminal Procedure Code provided by the respondent was too broad. Thus the SACL ruled in favour of privacy rights and stated that illegally obtained evidence may not be used to prove a disciplinary offence.

Another issue faced by Lithuanian courts has been the use of classified documents as proof in administrative proceedings. The Constitutional Court of the Republic of Lithuania has stated in its decision of 15 May 2007 that according to the Law on Administrative Proceedings the factual data comprising a state or official secret may be used as proof in administrative proceedings only when they are declassified according to the law, thus it is essentially forbidden to use classified

[4] http://www.teise.org/data/Teises_i_privatuma_uztikrinimo_problemos.pdf
[5] Case No. A3-750/2004 (9 November 2004)

data as proof. However, this prohibition is not absolute. Whether the factual data comprising a state or official secret in an administrative case is proof, is to be decided by the court taking all relevant circumstances into account. This must not depend on subjective factors. If there is sufficient non-classified data in order to decide on a case and to implement justice as required by the Constitution, the classified information (in order to protect the public interest) should not be a proof in the case and parties to the case may have no access to it. The court must assess whether it will be able to deliver justice without taking into account the classified data. The Constitutional Court also stated that a court decision must not be based only on the classified information that is not known to (one of) the parties to the case.

In this regard one should also note the decision of the European Court of Human Rights in case Gulijev v. Lithuania[6]. The applicant was refused renewal of a residence permit in Lithuania on the basis of a State Security Department's 'secret' file stating that he posed a 'threat to national security and public order'. Under domestic law factual data constituting State secrets were not to be used as evidence in administrative proceedings until they were declassified. The Court of Human Rights stated that Government had not provided the Court with further factual information substantiating why domestic authorities considered the applicant a threat. Although the applicant had a criminal conviction, it involved theft and not a crime related to national security. Accordingly, the applicant's deportation and prohibition from re-entering Lithuania, where his two children and wife lived, until 2099 had not been necessary in a democratic society, thus there had been a violation of the Convention.

The same reasoning was recently applied by the Supreme Administrative Court of Lithuania in case No. A-544-822/2015[7]. In this case the embassy of Lithuania had decided not to issue visa to the applicant based on a consultation of the State Security Department, even though this consultation had been classified. The SACL invoked the case-law of the European Court of Justice on that matter and decided that the court of first instance had to offer the respondent in the case to provide all the data about the applicant that it possessed, and to offer participants of the case to declassify the secret document or part of it. The SACL stated that because the reasoning of the State Security Department's consultation was not disclosed and further information with regard to the refusal to issue visa was not provided, it was not clear why the applicant had been estimated to pose a threat of illegal immigration. The non-reasoned decision could not be held legitimate and substantiated. The case was remitted to the court of first instance.

[6] Application No. 10425/03 (16 December 2008)
[7] 26 February 2015