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: Norway

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

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

(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

In Norway there is no administrative institution which is responsible for free access to information. The different public bodies are themselves responsible for giving the public access to information. If the applicant is denied access to information, he or she may complain to the authority superior of the public body which possess the required information. Then the superior authority will assess the request and make a decision. This decision may be brought to court in a normal court procedure which will be further described in question no. 2.

Hence, there is no authority in Norway which is responsible for a unified practice. However, the Parliamentary Ombudsman supervises maladministration and injustice on the part of public agencies. The Ombudsman normally works on the basis of complaints from citizens. A displeased citizen who has not been given access to the information he or she seeks, may make a complaint free of charge to the Parliamentary Ombudsman. The Parliamentary Ombudsman may criticise a public body if it has not taken care of its responsibility regarding free access to information. The Parliamentary Ombudsman has a high standing in Norway. A public body will seek to avoid critic from the Ombudsman and normally follow his recommendations.

Protection of personal data

In Norway the administrative authority for protection of personal data is the Norwegian Data Protection Authority. The Data Protection Authority had been established before Directive 95/46/EC, and was already performing most of the tasks the directive required.

The Data Protection Authority is according to the Personal Data Act an independent body. The main tasks of the Data Protection Authority are to keep a public record of all processing of personal data that is reported, or for which a licence has been granted, deal with applications for licences, receive notifications and assess whether orders shall be made in cases where this is authorized by law, verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies

are rectified. The Authority also identifies risks and provides advice and guidance for issues regarding personal data.

The Data Protection Authority may apply administrative sanctions like fines for severe infringement of the Act. The Authority also has the competence to apply coercive fines to secure compliance with an order given by the Authority.

The Personal Data Act also has a provision which make some of the gravest infringement of the Act a criminal offense.

There is also a provision in The Personal Data Act which states that the controller of the personal data shall compensate damage suffered as a result of personal data have been processed contrary to provisions in the Act. Hence, the Act can be used as basis for liability in a court case for damages.

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 procedure to get access to information possessed by a public body starts with a request to the respective body. If the applicant has requested information which is not obtained in a case where he is a party, the request is governed by the Act relating to the right of access to documents held by public authorities and public undertakings ("Freedom of Information Act"). If it is information in a case where he is a party there will apply regulations which give him more access than in accordance with the Freedom of Information Act. However this description will be restricted to the first category.

The request for information in accordance with the Freedom of Information Act can be both oral and written. The public body will assess the request and if the conditions by the law are fulfilled the information will be given without any further procedure. The public body has to give the applicant an answer within five days. If the public body has not given an answer within the time limit, the applicant can make a complaint to the superior body in accordance with the procedure for denials.

If the public body denies the request for access to information the public body has to do this in writing. The denial shall state the provision which is the basis for the denial and the reason why the provision is fulfilled. If the applicant is not satisfied with the reason for denial he or she can make a complaint to the public body's superior body. It is not possible to complain against a decision which gives access to the information.

The superior body will make an assessment of the complaint as soon as possible, normally within three weeks. The decision made by the superior body will be in writing, and will be the final document in the administrative procedure.

If the applicant was denied access to the information in accordance with the Freedom of Information Act section 32, he or she may bring the decision before the court. In Norway we do not have administrative courts, so the decision will be brought before the court of first instance. The decision to deny the access to information will be tried by the court with the same procedure as other decisions made by public authorities. This normally means that the court will assess whether there is a provision to deny access to the information, whether the authority based its assessment on the correct facts, and that the authority has made no procedural errors. The judgment given by the court of first instance can be appealed as other judgments to the Court of Appeal and in final instance to the Supreme Court. However, to get an appeal reviewed in substance before the Supreme Court, the appeal has to rise legal questions which are of importance to clarify.

As mentioned above, the applicant may complain against the denial of access to information also to the Parliamentary Ombudsman. He can not change the decision, but his critics and recommendations are, as mentioned in question no. 1, normally followed by the public body. A complaint to the Ombudsman is a faster and a much more cost efficient procedure than a court case. Hence, this may be why we in the Norwegian courts have very few cases regarding the right to information.

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

The Data Protection Authority, as mentioned above, gives orders of compliance and fines for infringements according to the Personal Data Act. The subjects affected by these decisions can make a complaint. A complaint made regarding a decision by the Data Protection Authority will be handled by the Privacy Appeals Board. This is a separate administrative appeal board for these cases, and can be seen as a form of specialised administrative court.

The decision made by The Privacy Appeal Board can be brought before the normal court system. The court procedure will be the same as stated above. The court of first instance will assess the decision regarding whether the decision is based on a correct legal provision, correct facts and whether the decisions has any procedural errors. In the same way as stated above the judgment from the first instance may be appealed both to the Court of Appeal and to the Supreme Court.

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 first legislative act regarding access to information was Act relating to public access to documents in the public administration of 19th June 1970. Before this act there was no general written legal basis for the public's access to documents held by a public body. However, in some laws on different legal areas there were already provisions which secured the public access to information.

The public authorities already, to a large extent, made information available to the public before the act was made. However, it was deemed adequate to make a legal basis for the practice for public access to documents from the different bodies, both to secure the public a right and to secure that the public authorities had a similar practice. Another reason was to make the right to free access to information more known to the public.

The first Freedom of Information Act was a result of a gradual expansion of access to information from different public bodies. The initiative of such an act came from a legislative reform. The process started with a report from the Freedom of Information Committee appointed by the Norwegian government. However, as early as in 1845 there had been proposed legislative acts that would give legal authority to the principle of freedom of information. The principle was also regularly part of the debate in Norway, and there were several committees that from time to time touched upon the theme.

The Freedom of Information Act of 1970 was amended several times and opened up for more access to information and a duty for the public body to consider the document for access even if it as a starting point was excepted from the right to access of information.

In 2006 a new Freedom of information Act entered into force. The new legislation was basically the same as the former one, but the Act was made easier to read for the public, more bodies like companies owned by the state or controlled by the state were included in the scope of the Act, and the applicant was given more rights in the case handling period.

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 Norwegian political system is probably to a large extent transparent compared to many other countries. As stated above, the public authorities already before the first Freedom of Information Act gave the public some access to information and there

already existed a legal principle about – however not a legal provision yet – that presumed access to information also for the public.

On the other hand, the Freedom of Information Act is a very important tool in Norway. It is important that the public has a legal right to information. First of all, this gives the public a trust in the public authorities. The public can see what and how the public authority handles different cases, and see that the authority normally can be trusted and treat everybody the same way.

However, it is not the public as each individual which is most important; the Freedom of Information Act also gives the press corps access to information. This is an important right in a democratic political system and is probably more important to the public's access to information on public authorities' work than the individual's right.

In addition the fact that the right to information is a legal right makes the public to a greater extent familiar with the right. They can find it in the law and it probably makes it more available. Of course it is also important that a public body can not deny the public access in a specific or difficult case. The Act will also secure that the public authorities have a uniform understanding of the principle of freedom of information. The legal right also secure that the decision made – in principle – can be brought before the court.

Another important factor in Norway is that the legal right to information can be reviewed by the Parliamentary Ombudsman. His advices and critics are not binding, but the high standing of the Ombudsman in Norway makes his critics something every public authority wants to avoid. Without a clear legal basis for the right to information this review by the Ombudsman would not be as effective as it is today. Hence, the legal basis for the right to freedom of information is of great importance in Norway.

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 appears above, our view is that freedom of information is such an important right in a democratic country that an application for information can not be seen as abuse. The Freedom of Information Act has exceptions for information of personal sensitive nature, business secrets and internal documents in the public authority; hence requests for information will not harm anyone and can not be seen as abuse. Even if there are several repetitive requests, the person only uses its right to freedom of information.

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 exception in Directive 95/46/EC can be seen as implemented in the Personal Data Act section 3. This provision restricts the objective scope of the Act. However, this provision only states that the King, in practice the government, can give administrative regulations regarding personal data for special activities and operations.

The Regulation of Handling of Personal Data excludes in section 1-2 the handling of personal data which is necessary as regards national security, relations with foreign states and other vital national security interests from the basic duties as described in the Act section 31 and 33. This means that the institutions and bodies which handle data included in the said exception, do not have to inform the Data Protection Authority about it, and the body or institution does not need a license to process sensitive personal data. The Regulation section 1-3 excludes cases handled in accordance with the laws regarding administration of justice, e.g. the Criminal Procedure Act, from the scope of the Personal Data Act.

The Regulation does not state which institutions or bodies the exception in section 1-2 will apply to. However, there is a formal order from the Ministry of Defence which regulates personal data for some institutions which indicates that those may benefit from the said exception. These institutions are The Norwegian Defence Security Agency (FSA) and the Armed Forces Joint Headquarters. The FSA's primary responsibility is the protective security service and operative security of the Armed Forces.

In the formal order for the Armed Forces, it is stated that there has to be legal basis in the Personal Data Act to get access to the information and that the information shall be handled in accordance with the Act. However, without a duty to inform, as stated above. The institutions have to establish internal control and not save the information for a longer period of time than necessary.

The Norwegian National Security Authority (NSM), The Norwegian Police Security Service, and the Norwegian Directorate for Civil Protection are also bodies which probably will benefit from the exception. However, the institutions will follow the regulations in the Personal Data Act for access to information, storage and erasing of information.

For the Norwegian Police Security Service the Police Register Act applies. This Act regulates the handling of personal data both for the police and the prosecuting authority. This Act has detailed regulations regarding the handling of personal data, and there are provisions that secure the person registered a right to know about the information if

secrecy is not necessary due to e.g. investigation. The Act consists of several legal safeguards like a right to access to information, a right to complain and supervision.

The Police Register Act does not provide any information regarding how the information is obtained. However, the regulations of how the police and the prosecuting authority obtain information are found in the Criminal Procedure Act and in the Prosecution Instruction. Information can be obtained by search of premises or personal body, detention, examination and other forms of investigation. However, of most interest to this question is surveillance and recording of telecommunication.

There is legal authority to do both surveillance and telecommunication control in the Criminal Procedure Act. There are severe conditions for the police to use such tools; first the court has to give its approval and there has to be a qualified suspicion of a grave criminal offence. The information obtained in this manner can normally only be used for the specific purpose. There are also regulations in the Act about the duty to give information to the person which as been subject to such control. There is also a specific provision regarding the police's duty to erase information obtained. It is also given a specific regulation regarding information obtained by surveillance or recording of telecommunication. This regulation gives specific provisions for how the information shall be obtained, how the information should be stored, and when and how the information shall be destroyed. All information deemed not relevant for the investigation shall be erased immediately and the same for information which can not be used as evidence in court, inter alia conversations with a lawyer.

For both the intelligence services and the police there are provisions demanding the bodies to report if they use any of the said tools. The respective laws prescribe controlling bodies which examine the reports to make sure that the actions are in accordance with the laws and regulations.

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.

We have not identified any special problems that emerge from this in our jurisdiction.