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: the Netherlands

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

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

(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

The right to free access to information is laid down in the *Wet Openbaarheid van Bestuur* (WOB) which deals with the regulation of administrative transparency in what are called "administrative matters" of governmental bodies. This concerns policy matters, both the preparation and the implementation thereof and only where this information has not been made public before. Governmental bodies are obliged to provide information both actively and passively (on request) concerning the fulfilment of their duties. The compliance of governmental bodies with the right to free access to information is not concentrated in one single authority such as an information commissioner. The WOB defines the governmental bodies that have an autonomous obligation to fulfil the requirements of the WOB. A number of governmental bodies are excluded from this obligation such as the Commission on whistle-blowers (*Commissie advies- en verwijspunt klokkenluiders*), the houses of Parliament and the Council of State.

Any person or organisation is entitled to request information from a governmental body either orally or in writing. The request has to be concrete. In case the request is send to the wrong governmental body, the latter is required to forward it to the correct body. The governmental body then has four weeks to decide whether or not to disclose the information. This period may be extended for another four weeks, though for environmental matters, the terms are shorter. The WOB defines a number of grounds for refusal, and draws a distinction between absolute grounds for refusal (e.g. information that could endanger the public safety or the unity of the government and information concerning personal data) and relative grounds for refusal (e.g. information that could endanger the relations with other States, the control and supervision tasks of administrative authorities or information that could interfere with the right to respect private and family life). In case of a relative ground for refusal the governmental body has to weigh the public interest of disclosing the information against the interest of protecting the specific ground for refusal. Internal policy views during deliberations are generally excluded from the area of application of the WOB. However, in view of a good democratic administration this information may be subject to disclosure as long as this in not traceable to the individual persons involved, in order to prevent interference with the right to respect private and family life.

The protection of personal data

In the Netherlands, the *College Bescherming Persoonsgegevens* (CBP) is appointed as the supervisory authority for the protection of personal data. The CBP was created by an Act of Parliament (*Wet Bescherming Persoonsgegevens WBP*) in accordance with the second chapter of Directive 95/46, Article 28. It enjoys the status of Independent Administrative Authority (*zelfstandig bestuursorgaan*), which means that although it is a governing body with public authority, in hierarchal terms, it is not a subordinate to the government or an individual minister. Its independence is guaranteed by law.[1] The minister is, however, entitled to some authority with regard to the position, composition and functioning of the CBP on general matters such as appointing members of the Advisory Board and providing policy guidelines concerning its powers to impose administrative fines.

The CBP enjoys both supervisory powers and advisory powers regarding the protection of personal data.

Its supervisory competence is not limited to that derived from the *Wet Bescherming Persoonsgegevens*, but stretches out to any law, decree or statutory provision that prescribes the processing of personal data, unless otherwise stated by law. There are many laws dealing with the protection and processing of personal data including the *Wet Politiegegevens,* dealing with police data, the *Wet Basisregistratie Personen*, dealing with the registration of persons by governmental bodies and the *Wet justitiële en strafvordelijke gegevens*, dealing with the processing of judicial data. A law that is excluded from the competence of the CBP is the *Wet op de inlichtingen- en veiligheidsdiensten 2002,* which is the legal basis for the Dutch secret services.

Its advisory powers are similarly broad. The government is obliged to present any draft bill or draft governmental decree that for an important part deals with the processing of personal data, to the CBP for advice. In regular cases, the CBP not only examines the draft bill or decree for its compatibility with the *Wet bescherming persoonsgegevens* but also for its compatibility with Article 8 of the European Convention on Human Rights. Furthermore, private and public parties can request the CBP for advice on the application of the *Wet bescherming persoonsgegevens* in specific cases. In some instances the CBP may give unsolicited advice to the government.

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.

Anyone can request information from a governmental body that is put down in documents. The procedure for such a request is defined partially in the WOB, but mostly in the Algemene wet bestuursrecht (Awb), the general administrative law act.

[1] Article 52, paragraph 2 of the Wet Bescherming Persoonsgegevens.

The governmental body has to decide on the request within four weeks. It can extend this term with another four weeks. If the citizen disagrees with the decision, it can object within six weeks. This objection is handled within the same governmental body, within six weeks. The governmental body is obliged to do a complete review of the request. It will send the citizen a decision on objection. If the citizen disagrees with this, it can appeal this decision in a court, again, within six weeks. The decision on objection has to specify which court has jurisdiction to handle the appeal. In principle, the court has to hold a hearing to deal with the appeal, for which both parties are invited. The court can give an oral decision right after the hearing, or a decision in writing within six weeks of the hearing. If a party disagrees with the court's decision, it can appeal to the Administrative Law Division of the Council of State. In most cases, the Administrative Law Division will hold a hearing for which the parties are invited. The Division can also decide to rule on the case without a hearing if both parties agree, or the ruling is obvious. A hearing of the Division is public. Afterwards, the Division will rule in the case, usually within six weeks. Its ruling deals with the question whether or not ruling of the court was correct. The rulings of the Division are made public.

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

The Administrative Law Division of the Council of State is one of the supreme courts in administrative procedures. It is therefore, a court of last instance in these cases. The Division has a role in deciding cases in which certain information, including personal data, are made public. The WOB knows specific grounds to withhold access to information that contains personal data. If the Division decides that a ruling of a court is not correct, it will annul this decision and come to another ruling. In that case it can decide to allow access to information that contains personal data, or it can also rule that certain information has to be refused on this ground. This is not only applicable in cases concerning a request based on the WOB, but also in other procedures that deal with access to governmental information, for example information that is gathered in criminal investigations. It is not possible to appeal a decision of the Division within the Dutch jurisdiction, it is the highest court. However, the Division has to abide by the rulings of the European Court of Human Rights and the Court of Justice of the European Union concerning this topic. The Division can ask the Court of Justice preliminary questions before it comes to a ruling.

Besides the WOB, Article 45 of the WBP gives citizens the right to appeal certain decisions that are made concerning data processing. These appeals follow the normal procedure laid down in the Awb, which is described above under 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.

Until the Second World War, the scope of the right to information was limited to the constitutional right of the parliament to be informed by the government. Policy with regard to the right to access to information for the general public was first developed after the Second World War, and was primarily based on the report of the Commission *Van Heuven-Goedhart*, that stressed the interest of informing the public but also warned for elements of propaganda when providing such information.

The discussion of introducing a bill concerning the right to access to government information started in the 1960s after a number of political affairs[2] concerning administrative transparency. This led to the installation of the *Commission-Biesheuvel*[3] that not only advised the government on how to reconsider its duty to inform the public, but also examined the options of introducing a bill dealing with freedom of information. Its report *Openbaarheid Overheid* was published in 1970 and included a draft bill that was based on the principle of good and democratic governance. Both the government and the Council of State were reticent about the proposals in the bill. The first Act of parliament, *Wet Openbaarheid van Bestuur* (WOB), dealing with the right of access to governmental information entered into force on May 1, 1980, albeit with a smaller scope than proposed by the *Commission-Biesheuvel*. The commission had recommended that internal governmental documents should be accessible by the public, but the government did not follow this recommendation. Only documents that are produced for external use are subject to requests based on the WOB.

In 1983, a new Article 110 was added to the Constitution. It states that the government in carrying out its public task has to strive for public access to information, in accordance with rules that are laid down by law. Further proposals were subsequently made, which were intended to include an enforceable fundamental right of access to information held by the government in the Constitution, but these have never been entered into Parliament.

The first WOB was evaluated by the *Commission-Van der Meij*, which report included 39 recommendations primarily addressing the need for a more generous regime on the right to access to information and a more active role of the government in providing information. Based on these recommendations, the WOB was revised in 1992. For the most part, the revision was more of a technical nature and did not lead

[2] The Faase affaire concerning a journalist that leaked information about the state budget and was subsequently denied access to ministries, and the Korsten affaire concerning a public relations agent paid for by the government.
[3] Commissie heroriëntatie overheidsvoorlichting.

to much substantive changes. Key provisions of the WOB have since not changed substantially.[4]

However, public debate on administrative transparency has since further been influenced by developments in European[5] and international law[6] and technological developments. The most notable development concerns the initiative to come to a new law concerning access to information held by the government that was presented in 2013 by Members of Parliament Voortman and Schouw and which includes the introduction of an information Commissioner. This proposal is currently under discussion by Parliament.[7]

The basic idea behind the WOB is a system of active disclosure. This means that governmental bodies should try to disclose as much information as they can. This idea is the reason that notions in the WOB about who is able to make a request, the form the request has to have etc. have always been interpreted in a broad sense by the courts, in order to allow disclosure of as much information as possible. For example, courts have ruled that the notion of documents in the WOB also includes videotapes, photographs, CD-ROMs, disc drives and other forms of digital information. A person requesting information is not obliged to state his interest in the information he would like to receive. The governmental body likewise is not allowed to base its decision whether or not to give the requested information on the possible interest of the requester.

Currently in the legislation, there is an article that states that if a governmental body does not decide on a request by a citizen within the timeframe that the concerning law prescribes, the governmental body has to pay a fine to the citizen. In case of the WOB, this has led to a number of requests that are not necessarily done in order to obtain certain information, but in the hope that the governmental organ would not be able to answer the request in time, therefore forfeiting the fine. This has led to a proposal by the government to change the legislation on this issue with regard to the WOB. This proposal is currently under debate by Parliament. It abolishes the automatic fine for the governmental body, but makes it possible for a citizen to ask a judge to impose a fine on the governmental body in case it takes too long to answer the request. The judge can then weigh the magnitude of the request (how much information is asked) and the importance for the requester on getting the information

[4] This does not include later amendments that further specified the type of governmental bodies that are required to comply with the WOB. Also, in 2005 changes were made to include specific provisions concerning the access to environmental information to implement the Treaty of Aarhus. Substantial changes were further brought to by implementing Directive 2003/98/EG on the re-use of public sector. Finally, the decision period has been widened after the coming into force of the *Wet dwangsom en beroep* that introduced the right to impose an order for period penalty payments in case the governmental body denies a request for information or exceeds the decision period.
[5] Directive 90/313/EEG concerning free access to environmental information and Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents
[6] Treaty of Tromso and the jurisprudence of Article 10 ECHR.
[7] Kamerstukken II 2013/14, 33 328.

quick (is it for a news article, or for a long research project for example) against the concerns for the governmental body.

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 free access to information is considered to be very important in the Dutch political system. It is used by news agencies and NGO's to get information about sensitive topics. In the public opinion, the importance of the right to free access of information is present. The fact that there is a proposal being discussed in Parliament to widen the scope of the WOB underlines this importance. When a previous Minister stated that he found that the scope of the WOB should be limited, a lot of organisations publically spoke out against this idea. The use of the WOB has also led to the revealing of scandals (for example in cases where political actors misused their right to claim certain expenses) and to cases where questions were raised on the policies that government was pursuing. An example of such a case was the debate on the use of electronic voting machines, where the NGO that was against the use of these machines actively used the WOB to get information on the decision making process with regard to this issue.

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 stated under question 4, most misuse of the WOB is linked to the fine that a governmental agency can forfeit when not deciding in time. A way people try to misuse the WOB is by requesting information that they can receive based on other laws by issuing a request based on the WOB. Examples of this are cases where someone gets a fine for speeding. Such a person has the right to access to the information that led to the fine (for example the photo of the traffic camera) based on the General Administrative Law Act (Awb). He can however also decide to request this information based on the WOB in hope that the decision by the governmental agency will be late. Since the processing of information regarding speeding tickets is cumbersome due to the large amount of data that needs to be reviewed in order to find the applicable data (traffic camera films), it is very likely that the governmental agency will answer the request after the deadline that is laid down in the law.

Other ways that abusers use are hiding WOB requests in more general letters to a governmental agency. Since the WOB doesn't prescribe a certain form to be used when asking for information, any question about information that lies with the agency can be considered a WOB request, even if this question is included in a document dealing with another issue (for example a job application letter).

In two recent judgements, the Division has ruled for the first time that such behaviour constitutes an abuse of rights and that in these cases; the governmental agency did not have to pay the fine.[8] As described under question 4, the government is working on changing the law on this topic.

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.

Article 7 of the Directive 95/46/EC is implemented through Article 8 of the *Wet Bescherming Persoonsgegevens* (WBP) and contains a limited list of grounds that justify the processing of personal data. This Article further emphasizes that any processing of data is justified only if it meets the criteria of proportionality and subsidiarity.

Administrative authorities or defence institutions with authority in the field of security or law enforcement base their powers to process personal data on other, more specific laws (lex specialis) such as the Politiewet (Police Act), the Wet Politiegegevens (Act on police data), the Wet Justitiële en strafvorderlijke gegevens (Act concerning judicial and criminal data) and the Wet op de inlichtingen- en veiligheidsdiensten 2002 (2002 Act on intelligence and security services). The WBP therefore, does not apply to administrative authorities that base their power to process data on these and other more special Acts that are listed in Article 2 of the WBP.

Most recently, the European Court of Justice gave a preliminary ruling on a number of cases referred to by the Administrative Law Division of the Dutch Council of State concerning the processing of biometric data, which included a question relating to the application of Directive 95/46/EC.[9] The question was raised in cases concerning the issuing of passports and identification cards that required fingerprints. However, the question concerning the application of Directive 95/46/EC was asked only within the context of Regulation (EC) nr. 2252/2004, and because the Regulation was not applicable in the particular cases, the European Court of Justice did not consider the Directive in its reasoning.

Article 7 (e) of the Directive is implemented through Article 8 (e) of the WBP with slight adjustments to correspond with the nature and terminology of the Dutch administrative law system. The exception provided for in Article 7 (e) is directed at administrative authorities in the performance of their activities governed by public law. The use of the term administrative authorities in the Dutch administrative law system, allows this exception to also be applicable to private parties that act within the limits of the administrative powers conferred upon them, such as a private schools in performing their administrative task of handing out diploma's. For the most part, however, this article is applied by governmental bodies, although only in the performance of their activities governed by public law. The sale or purchase of real estate by governmental bodies for example, is excluded for the application of this

[8] The Administrative law Division of the Council of State, November 19, 2014, case nr. 201311752/1/A3.
[9] European Court of Justice, April 16, 2015, C-446/12, C-447/12, C-448/12 and C-449/12.

article. The key concepts of this provision “administrative authorities” and “administrative powers”, therefore, have autonomous meaning.

The general prohibition of Article 8 (1) of Directive 95/46/EC is implemented in Article 16 of the WBP. Additional exceptions to those listed in Article 8 (2) of the Directive, are implemented in the second paragraph of chapter two of the WBP (Articles 16-24), as provided for in Article 8 (4) of the Directive. These include exceptions to process data concerning race (Article 18), political opinion (Article 19), membership of a trade union (Article 20) and health (Article 21).

Article 18 of the WBP only allows data concerning race to be processed for identification purposes or affirmative action policy. The processing of data about political opinion is only allowed for the purpose of appointing persons in public administration such as mayors. The exception for processing data concerning membership of a trade union only applies to labour union federation to which the labour union itself is connected to. Probation and after-care institutions can benefit from the exception concerning the processing of health data.

The more special laws for administrative authorities in the field of security and law enforcement, the Wet op de inlichtingen- en veiligheidsdiensten 2002 (Article 13 sub 3 and 4), the Wet Justitiële en strafvorderlijke gegevens (Article 39c, sub c), and the Wet Politiegegevens (Article 5), allow data concerning race, political opinion, health, sex life, religion and membership of trade unions only to be processed in addition to the main purpose of processing personal data and only if the processing of the specific data is inevitable.

Article 8 (5) of the Directive is implemented in Article 21 and Article 22 of the WBP that provide the general exception for administrative authorities who work in the field of security and law enforcement. Article 22 of the WBP specifically concerns the processing of personal data related to criminal convictions and justified suspicions of criminal acts. It contains a general exception for administrative authorities that have the administrative power to enforce criminal law, including those who are empowered to do so based on special laws such as the Politiewet (Police Act) and the Wet Justitiële en strafvorderlijke gegevens (Act concerning judicial and criminal data).

In the Netherlands the complete register of criminal conviction is kept under the control of the Board of Procurer Generals.

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.

There are different pending cases at the Division that deal with the refusal of municipalities to give a person a passport or ID card because this person refuses to give the necessary fingerprints. The Division has asked the Court of Justice if this obligation to give fingerprints, that finds it origin in EU-law, is in accordance with the right to privacy. The Court has answered this is the case and that fingerprints can be collected for this means (see under question 7).

Other issues in this area deal with information resting with law enforcement agencies and the national security agency. For certain professions, a declaration concerning behaviour is necessary (for example for government employees with access to secure information, but also for people working with young children). Such a declaration can be refused if a person is listed in the Police registry data. However, if this data is part of an ongoing investigation, the data may not be released to the person in question. He is then only informed that his declaration is refused, without being given access to the data that has led to the refusal.

A final issue is that of data retention and the question if security and law enforcement institutes are allowed to accumulate and process bulk data. The Court of Justice has struck down the Data retention directive.[10] In the Dutch debate, the question is whether or not this processing of bulk data in view of the advantages for criminal investigations should be allowed, or that the collection and processing of data should be limited and subject to strict conditions.

[10] European Court of Justice, April 8, 2014, joined cases C-293/12 en C-594/12.