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: Germany

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

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

Germany

(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.

Federal Commissioner for Data Protection and Freedom of Information

With regard to the latest case-law of the Court of Justice of the European Union (CJEU) [1] the Federal Data Protection Act has recently been amended[2] to further strengthen the independence of the Federal Commissioner for Data Protection. The institution has been altered into an independent supreme federal agency („oberste Bundesbehörde"), which is neither personnel-wise nor organisationally linked to other governmental institutions. In addition, it is no longer subject to any legal or functional supervision by the Federal Government. The Federal Commissioner of Data Protection is elected by parliament and appointed by the Federal President. Against his or her will the Federal Commissioner of Data Protection can only be dismissed by the Federal President for reasons that justify the dismissal of a judge appointed for life.

Anyone considering their right to access to information to have been violated may appeal to the Federal Commissioner. Public bodies of the Federation are obliged to support the Federal Commissioner and his/her assistants in the performance of their duties, especially by granting information in reply to their questions, the opportunity to inspect all documents connected with the monitoring and access to all official premises at any time.

Should the Federal Commissioner discover infringements of the respective provisions or other irregularities, he/she shall lodge a complaint with the competent supreme federal authority or the relevant representative body and – if applicable – inform the competent supervisory authority. Additionally, he/she requests a statement by a date which he/she determines. The statement to be delivered is also supposed to describe the measures taken as a result of the Federal Commissioner's complaint.

---

[1] Court of Justice of the European Union (Grand Chamber), Judgement from 16th October 2012 – C-614/10.

[2] Second Law to Amend the Federal Data Protection Act, 25th. February 2015, coming into effect on 1st January 2016

The Federal Commissioner for Data Protection and Freedom of Information submits an activity report to the Bundestag every two years. Such report informs the Bundestag and the public on key developments in the field of data protection and freedom of information.

Each Federal State has its own Data Protection Commissioner who also performs the function of Commissioner for Freedom of Information if a State law on freedom of information has been passed. Most Federal States have already implemented the CJEU´s decision concerning the independence of the data protection authority earlier since their legislation required a more comprehensive amendment to European standards. For example, in some states the Data Protection Commissioner's competence encompassed only data protection compliance of state agencies and other public-law governed institutions. In contrast supervising data processing by private bodies (including public enterprises), which falls into the legislative powers of the states, was considered primarily a matter of commercial administrative law. Here, tensions were identified between the independence of the Data Protection Agency on the one hand and the democratic foundation and control of administrative action on the other hand. In consequence, in some states the data protection authority for the private sector was established directly at a state ministry; in other states it did fall within the scope of the State Data Protection Commissioner`s competence, however the Commissioner not acting with the same degree of independence that was provided for in relation to the public sector. At least since the CJEU released its decision legislation has changed. State Data Protection Commissioners are now competent to monitor and to control both public and private sector and their institutional and personal independence applies in both areas. State Data Protection Commissioners are elected by parliament, partly by a qualified majority. In most cases legal supervision rests on the head of parliament.

Competences and functional responsibilities in monitoring data protection compliance are divided between the Federal Commissioner for Data Protection (and Freedom of Information) and sixteen State Data Protection Commissioners. The Federal Commissioner shall monitor compliance by federal public agencies. Its control also covers personal data obtained by federal public agencies concerning content and specific circumstances of correspondence, postal communication and telecommunication as well as personal data subject to professional or official secrecy, especially tax secrecy.[3] State Commissioners shall monitor compliance with data protection laws of the states by public agencies of the states (including municipal and other institutions under public law on the state level) and the data processing by private bodies and public enterprises.

State Commissioners for Data Protection are not subject to any form of supervision by the Federal Commissioner for Data Protection. However, conferences of both state and

[3] See Art. 24 Federal Data Protection Act.

federal actors are held periodically to coordinate interests and to the exchange experiences. These conferences have an advisory status only – similar to the working party due to Art. 29 Data Protection Directive. Participation is optional. They have no legal basis in the Code of Data Protection or other laws.

So-called Data Protection Officers play a special and – de facto – important role in securing data protection compliance. They are part of an additional means of self-regulation of the private data processing sector. Data Protection Officers shall – roughly described – be appointed by all public and private institutions which process personal data automatically (with an exception for small units).[4] Only people with specialized knowledge and who have demonstrated the required reliability for performing the duties concerned may be appointed. Data Protection Officers shall be directly subordinate to the head of the institution He or she is not independent in a strict sense, however he or she shall be free to use his or her specialized knowledge in the area of data protection and shall not suffer any disadvantages by performing his or her duties. Data Protection Officers shall ensure compliance with this Act and other data protection provisions. For this purpose, Data Protection Officers may consult the competent authority responsible for data protection control .[5] Data Protection Officers are neither administrative officials nor otherwise linked to the Data Protection Commissioner. In particular, Data Protection Officers are by no means subject to any kind of directives or at least supervision by the Data Protection Commissioner. However, in practice there is a chance of cooperation between Data Protection Officers and the Commissioner for Data Protection, which might promote the idea of data protection in both public and private institutions dealing with personal data.

Free access to information

In Germany, the authorities of the Federal Government shall grant access to official information to everyone in accordance with the provisions of the Freedom of Information Act.[6] Other Federal bodies and institutions have the same obligation insofar as they discharge administrative tasks under public law. Even a natural or legal person shall be treated as equivalent to an authority where an authority avails itself of such a person in discharging its duties under public law.

Due to Germany's federal structure the access to information from the authorities of the Federal States ("Länder") is regulated by the States themselves. 11 Federal States[7] have

[4] See Art. 4f Federal Data Protection Act.

[5] See Art. 4g Federal Data Protection Act.

[6] See Art. 1 of the Freedom of Information Act (see http://www.gesetze-im-internet.de/Teilliste_translations.html for English versions of German legislation).

[7] Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Western Pomerania, North Rine-Westphalia, Rhineland-Palatinate, Saarland, Saxony-Anhalt, Schleswig-Holstein, Thuringia.

enacted statutes relating to the freedom of information or even more far-reaching ones (see also question four below).

An authority's decision to reject an application for access to information in part or in its entirety can be challenged by lodging an administrative appeal and bringing an action to compel performance of the requested administrative act (see question two for details).

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 following remarks refer only to German Federal law.

Free access to information

The authority which is authorised to dispose of the requested information decides on the application for access to information. However, there are several restrictions by law to the right to free access to information.[8] There are not only various statutory exceptions provided for in the Freedom of Information Act regarding the protection of special public interests (see question four below), but also for personal data and intellectual property. Access to personal data[9] may only be granted where the applicant's interest in obtaining the information outweighs the third party's interests warranting exclusion of access to the information or where the third party has provided his or her consent. Special types of personal data may only be transferred subject to the express consent of the third party concerned. The applicant's interest in accessing information shall not predominate in the case of information from records relating to the third party's service or official capacity or a mandate held by the third party or in the case of information which is subject to professional or official secrecy. No entitlement to access to information applies where such access compromises the protection of intellectual property. Access to business or trade secrets may only be granted subject to the data subject's consent.[10]

Where an entitlement to partial access to information applies, the appurtenant application is to be granted to the extent to which information can be accessed without revealing information which is subject to confidentiality or without unreasonable administrative expenditure.[11] The information is to be made accessible to the applicant forthwith, with due regard to his or her interests. Access to the information should be provided within one month.

[8] See Art. 3 to 6 of the Freedom of Information Act.
[9] See Art. 5 of the Freedom of Information Act.
[10] See Art. 6 of the Freedom of Information Act.
[11] See Art. 7 of the Freedom of Information Act.

The authority has to grant a third party whose interests are affected by an application for access to information opportunity to submit a written statement within one month when there are indications that the said third party may have an interest warranting exclusion of access to the information.[12] In those cases the decision shall be provided in writing and shall also be notified to the third party.

Decision on the denial of a request and preliminary proceedings

In cases in which the authority rejects the application in part or in its entirety[13], it is to provide notification as to whether and when partial or full access to the information is likely to be possible at a later juncture. The application may be rejected where the applicant is already in possession of the requested information or can reasonably be expected to obtain the information from generally accessible sources. It is permissible to challenge the decision to reject the application by lodging an administrative appeal and bringing an action to compel performance of the requested administrative act. A complaint may also be filed regarding the ruling on the costs for the disclosure of information.

The objection shall be lodged with the authority which has carried out or rejected the administrative act within one month after the respective announcement to the aggrieved party. If the authority considers the objection to be well-founded, it will remedy it. If the authority does not remedy the objection, a ruling on the objection is to be handed down. This will be issued by the next higher authority or if the next higher authority is a supreme federal authority, the authority which has issued the administrative act.

Court procedure – general introduction

In principle, the applicant can challenge the rejection of a request by means of an enforcement action while a third party whose interests are affected might bring a rescissory action against a decision to grant access. Pursuant to the provisions of the Code of Administrative Court Procedure, these actions must be lodged within one month of service of the ruling on the objection.

A lawsuit starts in the administrative courts of first instance. The Higher Administrative Courts are courts of appeal (appeal on points of fact and law). The access to appeal depends on leave to be granted either by the administrative court which rendered the judgment in first instance or by the court of appeal. The appeal on points of fact and law is only admissible if serious doubts exist as to the correctness of the judgment, if the case has special factual or legal difficulties, if the case is of fundamental significance, if the judgment derogates from a ruling of higher courts and is based on this derogation, or if a

[12] See Art. 8 of the Freedom of Information Act.
[13] See Art. 9 of the Freedom of Information Act.

procedural shortcoming applies on which the ruling can be based.[14] When leave to appeal is once granted, the Higher Administrative Court will fully re-examine the factual and legal issues of the case. The proceedings correspond more or less to the proceedings in the first instance.

If the legal interests of others are affected by a ruling, the court may subpoena them ex officio or on request.[15] In the field of access to information this might be the case e.g. for third persons whose interests are affected by an application for access to information.

Role of the Federal Administrative Court (appeal on points of law)

The Federal Administrative Court reviews the decisions of the lower courts only on points of law. It is bound to the facts established in the judgment to be reviewed. Generally, the actions brought before the Federal Administrative Court are directed against decisions of the courts of appeal. With the consent of both parties, however, it is also admissible to bypass the remedy of appeal and to challenge the ruling of a court of first instance directly before the Federal Administrative Court.

Appeals on points of law have to be granted either by the court issuing the judgment in dispute or – initiated by a complaint against non-admission – by the Federal Administrative Court itself. They are only admissible if the legal case is of fundamental significance, the judgment deviates from a ruling of the Federal Administrative Court or of the Federal Constitutional Court, *inter alia*, and is based on this deviation, or a procedural shortcoming applies on which the ruling can be based.[16] While appeals at the Higher Administrative Court of a certain Federal State ("Land") may be based both on the infringement of laws of that Federal State or on the violation of Federal Law, appeals at the Federal Administrative Court may be based on infringements of Federal Law only (see also question four below).

Interim procedure

Apart from these regular actions the Code of Administrative Court Procedure provides for interim injunctions and other provisional measures in order to guarantee the effectiveness of judicial protection in urgent cases.[17] On request, the court may, even prior to the lodging of an action, make an interim order in relation to the subject-matter of the dispute if the danger exists that the enforcement of a right of the plaintiff could be prevented or considerably impeded by means of an alteration of the existing state. The interim order allows an applicant to make preliminary provision for the legal position until a decision can be reached in the main action. As such orders often must be made within a very short time, procedural requirements are less strict than those for the main action. In

[14] See Art. 124 of the Code of Administrative Court Procedure.
[15] See Art. 65 of the Code of Administrative Court Procedure.
[16] See Art. 132 of the Code of Administrative Court Procedure.
[17] See in particular Art. 123 of the Code of Administrative Court Procedure.

order to obtain an interim injunction deciding the fundamental question, the applicant has to establish that the court's main procedure cannot be concluded in time, and that the main proceedings probably will lead to a final decision in his favour. However, the decision may only be temporary in effect, it therefore may not make a decision in the main action superfluous.

As a basic principle, interim orders which forestall the decisions on the main issue or amount to the disposal of the main dispute will not be passed by the courts. Thus an administrative authority normally will not be compelled to take the requested action by interim procedures because this would amount to a final decision in the main action. Requests for information are, by definition, granted by providing the information. Passing an affirmative interim order in such cases would therefore regularly lead to a definite decision. That is why interim procedures will rarely be successful in cases regarding the free access to information.

Decisions ordering interim measures in exceptional cases may still lead to a definite decision on the fundamental question, if otherwise no effective remedy would be possible. That is the case if the applicant, in waiting for the final judgment, would suffer a violation of rights impossible to correct or to compensate adequately afterwards. Accordingly, for example a Higher Administrative Court[18] passed as an exception to the basic principle an interim order forestalling the final decision in the main action in a case concerning the Law on Environmental Information that is insofar comparable to the Freedom of Information Act. The applicant in this case had to urgently introduce the requested information into other judicial proceedings in order to exercise his rights properly before a final decision could have been reached in the case on access to information.

In-camera procedure[19]

The Code of Administrative Court Procedure obliges the administrative authorities to submit to the court all certificates or files, to transmit electronic documents and provide information relevant to the case. The parties can inspect the court files and the files submitted to the court.

If the knowledge of the content of this data and documents would prove disadvantageous to the interests of the Federation or of a Federal State, or if the events must be kept strictly secret for other reasons, the competent supreme supervisory authority may refuse

[18] Order of the Higher Administrative Court of Berlin-Brandenburg of the 14th May 2012 – OVG 12 S 12.12 – http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/ehb/bs/10/page/-sammlung.psml?doc.hl=1&doc.id=MWRE120001615&documentnumber=19&numberofresults=32&showdocca se=1&doc.part=K&paramfromHL=true#focuspoint.

[19] See Art. 99 of the Code of Administrative Court Procedure.

the provision of the data and documents. If the authorities refuse to disclose certain data and documents, the Higher or the Federal Administrative Court finds by order whether the refusal is lawful. Therefore the court which has jurisdiction for the main case assigns the application for such a procedure of the party concerned and the main case files to the adjudication bodies with special jurisdiction (special senates). The supreme supervisory authority shall provide the data and documents refused on request by this panel of judges. The parties' right to inspection does not apply to the files and electronic documents submitted in accordance with the in-camera procedure. The members of the court shall be obliged to maintain confidentiality; the grounds for the decision may not provide an indication of the nature and content of the secret certificates, files, documents and information.

The provisions regulating the in-camera procedure do not give the claimant a right to demand a court's order requesting the authorities to disclose specific files or information. The procedure is only designated to decide whether an administrative refusal to comply with court orders is justified or not. The special senates do not decide on the merits.

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

The general rules and principles of court procedures described in the previous answer apply also to data protection cases. There are no specific rules and options concerning data protection.

The Federal Administrative Court is the Supreme court in general administrative matters except those within the jurisdiction of tax courts and or social security courts (special administrative courts). Data protection matters are not subject to an exclusive jurisdiction of one of the five branches of jurisdiction in Germany. Data protection compliance is a cross-sectional matter. Questions of law may arise in any branch of jurisdiction. Social security courts – for example – decide questions of social data protection, labour courts are competent if personality rights of employees are at issue.

Decisions of the Federal Administrative Court are final. The mere remedy left is a constitutional complaint to the Federal Constitutional Court. However, this is an extraordinary remedy to allege a violation of national constitutional law only. Neither a violation of the Data Protection Act nor a violation of Directive 95/46/EC, Art. 8 Charter of Fundamental Rights of the European Union or Art. 16 Treaty on the Functioning of the European Union can be invoked. The federal constitution[20] does not provide for an explicit right of data protection. However, the Federal Constitutional

[20] Several State Constitutions know an explicit „Right for Data Protection" (for example Art. 33 Constitution of Saxony).

Court has developed a „right to informational self-determination“[21] as part of the general right of personality, which protects an individual`s right to decide on his or her personal data. This concept is slightly different from the concept of „privacy“ and emphasizes the importance and significance of data protection for personal autonomy and personality.
As the Federal Administrative Court is a court of last resort, against whose decisions there is no judicial remedy under national law, it has to bring matters before the CJEU, if a question is raised concerning the validity or interpretation of acts of the European Union (Art. 267 Treaty on the Functioning of the European Union). Even though the Data Protection Directive is now in force for almost twenty years and has largely harmonized protection of personal data in the European Union, the Federal Administrative Court has not yet made a request for a preliminary ruling in data protection matters. One of the reasons is to be seen in the small number of cases concerning federal laws on data protection (most of the cases brought before administrative courts concern activities of state authorities and are hence to be decided under state law). Moreover, the Federal Constitutional Court has implemented an intensive control on national laws constraining the constitutional right to informational self-determination. Anyhow, lower administrative courts requested preliminary rulings by the CJEU concerning the central register for foreign nationals,[22] the publication of information on beneficiaries of agricultural aid[23] and security features and biometrics in passports and travel documents.[24] Another request of the Federal Court of Justice is still pending.[25]

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.

<u>Influence of the constitutional background on free access to information</u>
Article 5 sec. 1 of the Basic Law only guarantees freedom of opinion, expression, and information, *inter alia*.[26] Regarding to the latter, every person has the right to inform him-

[21] See the basic Judgement of Federal Constitutional Court of 15th Dezember 1983 – 1 BvR 209/83 et. al. – BVerfGE 65, 1 („Volkszählung“).
[22] See Court of Justice of the European Union, Jugdement 16th December 2008 – C-524/06 (Huber) (Higher Administrative Court of Northrhine-Westfalia).
[23] See Court of Justice of the European Union, Jugdement 9th November 2010 – C-92, 93/09 (Schecke and Eifert) (Administrative Court Wiesbaden).
[24] See Court of Justice of the European Union, Judgement 17th October 2013 – C-291/12 (Schwarz) (Administrative Court Gelsenkirchen).
[25] Federal Court of Justice, Decision 28th October 2014 – VI ZR 135/13 (Is a dynamic InterProtocol-Number as a personal data in the sense of Art. 2 lit. b Directive 95/46[EC])?); a former request concerned Directive 2002/58/EC (see Court of Justice of the European Union, Jugdement 22th November 2012 – C-119/12 [Probst]).
[26] In German: See judgement of the Federal Constitutional Court of 24th January 2001 – 1 BvR 2623/95, 1 BvR 622/99 – http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2001/01/-

/herself without hindrance from generally accessible sources. An information source is generally accessible if it is technically suitable and determined to provide information to the public.[27] The entitlement to access to information may only be derived from statutory law. The Freedom of Information Acts of the Federation and the Federal States are such statutory law.

The Federation itself is competent to regulate the access to information from the authorities of the Federal Government as a matter which, logically, can only be decided at federal level. The Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act) was passed on this basis on the 5th September 2005. Inversely, the Federal States have the competence to legislate the access to information from the State authorities. Ten States have enacted their own Freedom of Information Acts while one State has even passed a Transparency Act which encompasses a duty to actively add information to a centrally managed, electronic and universally accessible information register (duty to publish).[28]

Historical development of access to information in Germany

Political initiatives promoting the introduction of freedom of information legislation had been existing in Germany at least since 1980.[29] Although these political trends emanated from different parties and groups of political players, they had not been able to prevail for a long time.

The State of Brandenburg enacted the first Freedom of Information Act in Germany in 1998 with a social-democrat-led government. This law was based on the State constitution which entitles everyone to inspect documents and other official information from the State authorities in Brandenburg.[30] The Brandenburg constitution was adopted only in 1992 after the re-establishment of this East-German State. This might have formed a reason for the enactment of such a unique provision. That way, ideas of the East-German civil rights movement which accompanied The Change ("Wende") in the former German Democratic Republic, might have found their way into the constitution.

The second State Freedom of Information Act was passed by the State of Berlin (conservative-social-democratic coalition) in 1999, followed by the State of Schleswig-Holstein (social-democratic-green coalition) in 2000.

---

rs20010124_1bvr262395.html recital 55, and order of the Federal Constitutional Court of the 9th February 1994 – 1 BvR 1687/92 – https://openjur.de/u/200577.html recital 13.

[27] In German: See order of the Federal Constitutional Court of the 9th February 1994, ibid.

[28] In German: Hamburgisches Transparenzgesetz (HmbTG) of the 19th June 2012 (http://www.hamburg.de/transparenzgesetz/).

[29] In German: See in detail Kollbeck/von Dobeneck, in: Berger/Roth/Scheel, IFG, 2006, Einl recitals 38 ff.

[30] Art. 21 sec 4 of the Constitution of the State of Brandenburg of the 20th August 1992 (http://bravors.brandenburg.de/de/gesetze-212792#21).

Parts of the East-German civil rights movement joined the Green Party in 1993, whereupon both of them formed the new party Bündnis90/Die Grünen and kept being involved in the issue of free access to information. Consequently, they were the first to introduce a bill for a Federal Freedom of Information Act to the German parliament ("Bundestag") in 1997.[31] Having taken over from a conservative-liberal coalition in 1998, the new social-democratic-green government coalition attended to the issue and introduced a ministerial draft bill in the year 2000.[32] In the year 2004, the parliamentary groups of the governing coalition introduced their own bill to the Bundestag after irreconcilable differences of opinion between them and the federal government had occurred on the issue. The Bundestag finally passed this law[33] with the votes of the governmental coalition against the votes of conservative parties and notwithstanding the abstention from voting by the liberal party.[34]

The enactment of the Hamburg Transparency Act was preceded by a popular initiative ("Volksinitiative") as first step of people's legislation, initiated by groups within civil society such as Transparency International, Mehr Demokratie (*more democracy*) and Chaos Computer Club. Before a petition for a referendum ("Volksbegehren") – the second step of people's legislation – could be initiated the Hamburg City Parliament ("Bürgerschaft") adopted the bill and passed the law with minor modifications and the consent of all fractions.

Milestones of jurisprudence

Even though the driving forces for freedom of information in Germany originated from legislature, they were followed by some remarkable steps taken by judiciary. Since the Federal Administrative Court is – as far as relevant in this context – only responsible for appeals on points of law which may only be predicated on the impugned judgment being based on a violation of federal law, the here presented case law will only deal with the Federal Freedom of Information Act.

Given that the access to information provided by the Federal Freedom of Information Act is unconditional, legal disputes largely have arisen from the scope of application of the law and various statutory exceptions.

The Freedom of Information Act grants free access to official information from the authorities of the Federal Government and other Federal bodies and institutions insofar as they discharge administrative tasks under public law.[35] The question whether Federal Ministries are to be classified as such authorities or bodies was brought before the Federal

[31] In German: BT-Drs. 13/8432 (http://dipbt.bundestag.de/doc/btd/13/084/1308432.pdf)
[32] In German: See in detail: Schoch, IFG, 2009, Einl recitals 122 ff.
[33] In German: BT-Drs. 15/4493 (http://dip.bundestag.de/extrakt/15/019/15019585.html).
[34] In German: Plenarprotokoll 15/179, p. 16959 (B).
[35] See Art. 1 para 1 of the Freedom of Information Act.

Administrative Court. Their obligation was disputed because it was argued that governmental work of a Federal Ministry (e.g. preparation of bills) cannot be regarded as administrative task. The Federal Administrative Court affirmed though their administrative task because the Freedom of Information Act does not draw a distinction between administrative and governmental work. [36] The Court argued that the purpose of the law would not be met properly if the Freedom of Information Act was not applicable to governmental work of the Federal Ministries which may be fundamental for civil society.[37]

In order to protect special public interests, the entitlement to access to information provided for by the Freedom of Information Act[38] does not apply where disclosure of the information may have detrimental effects on e.g. international relations, certain military interests, internal or external security interests, monitoring or supervisory tasks of the financial, competition and regulatory authorities, matters of external financial control, measures to prevent illicit foreign trade, the course of current judicial proceedings and a person's entitlement to a fair trial or the pursuit of investigations into criminal, administrative or disciplinary offences. Furthermore, access will not be granted in cases where e.g. disclosure of the information may endanger public safety, where and for as long as the necessary confidentiality of international negotiations or consultations between authorities are compromised, where the information is subject to an obligation to observe secrecy or confidentiality or where the information is subject to professional or special official secrecy, where disclosure of the information would be capable of compromising fiscal interests of the Federal Government in trade and commerce, and finally with regard to the intelligence services and the authorities and other public bodies of the Federal Government, where these perform comparably sensitive duties.

These various statutory exceptions regarding the protection of special public interests, but also those relating to personal data[39] and intellectual property[40] (see question two above) are to be construed narrowly pursuant to the rulings of the Federal Administrative Court.[41] An all-embracing exemption from the entitlement to access to information was only approved for the intelligence services and the authorities and other public bodies of the Federal Government, where these perform comparably sensitive duties.[42] The Federal

---

[36] In German: Judgment of the Federal Administrative Court of the 3rd November 2011 – 7 C 3.11 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=031111U7C3.11.0, principle 1 and recital 10.
[37] Ibid. p. 128, recital 20.
[38] See Art. 3.
[39] See Art. 5 of the Freedom of Information Act.
[40] See Art. 6 of the Freedom of Information Act.
[41] In German: Last mentioned, *inter alia,* in the judgments of the Federal Administrative court of the 27th November 2014 – 7 C 12.13 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=-271114U7C12.13.0, recital 24 and – 7 C 20.12 – recital 27.
[42] In German: Judgment of the Federal Administrative Court of the 24th May 2011 – 7 C 6.10 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=240511U7C6.10.0, recital 13. See also Art. 3 No 8 of the Freedom of Information Act.

Administrative Court, however, rejected a generalising view on further exclusion rules of Art. 3 of the Freedom of Information Act and therefore the existence of further all-embracing exemptions.[43] Rather is it considered necessary by the Court to determine the specific possibility of detrimental effects that might lead to a refusal of access. Therefore, the obliged authority has to state the facts which suggest the possible impairment of the protected interests in every single case.[44] The protected interests have to be concretely and seriously endangered.[45] If a sufficient danger cannot be established for all information in demand, access to the information left has to be granted. The question whether and to what extent detrimental effects can be assumed is subject to full judicial review. Only one exemption to this rule has been accepted: The Federal Administrative Court has left a margin of appreciation ("Beurteilungsspielraum") only to authorities that can refuse access to information where disclosure of the information may have detrimental effects on international relations.[46] This is due to the fact that the Basic Law gives broad leeway to the Federal Government for the conduction of relations with foreign states.

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 Federal Administrative Court has emphasised in its rulings that the spirit of the Freedom of Information Act is aimed not only at the effective exercise of civil rights advanced by improved administrative transparency, but also at promoting the process of shaping the democratic will and public opinion as well as the improvement of the control of public action.[47]

The cases decided on by the Federal Administrative Court were related to applicants who requested access to information predominantly for the purpose of the formation of public opinion. Journalists in particular tried to obtain information that exceeds that obtainable by reference to the freedom of the press. Persons and organisations like authors, historians, associations or engaged citizens have also tried to get information beyond that which can be accessed via particular remedies (e.g. from laws on archives, public records or registers). Furthermore, companies and other market players make use of the right of access to information in order to obtain information of economic interest. Finally, there

[43] In German: Judgment of the Federal Administrative Court of the 15th November 2012 – 7 C 1.12 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=151112U7C1.12.0, recital 41.
[44] Ibid.
[45] In German: Order of the Federal Administrative Court of the 18th July 2011 – 7 B 14.11 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=180711B7B14.11.0, recital 11.
[46] In German: Judgment of the Federal Administrative Court of the 29th October 2009 – 7 C 22.08 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=291009U7C22.08.0, recitals 13 ff.
[47] In German: Judgment of the Federal Administrative Court of the 27th November 2014 – 7 C 20.12 – http://www.bverwg.de/entscheidungen/entscheidung.php?ent=271114U7C20.12.0, recital 27.

are cases where private persons and companies take advantage of the entitlement to information in order to substantiate their assertion in other (potential) lawsuits (especially actions for damages or official liability claims).

Our experience so far has demonstrated that authorities which reject requests for access to information often worry that granting access could hinder the effective functioning of the authority itself. This is because screening, selection and provision of the requested information may impose a heavy workload on the obliged authorities especially in the case of a considerable number of files. This kind of additional administrative work and expenditure can also emerge from the existence of many documents which have a sensitive character or are subject to confidentiality. Another reason for a restrictive attitude of authorities seems to be the misgiving that third parties might not provide information to authorities voluntarily any more as they could fear that this information potentially will not be kept confidential in future but rather has to be provided to the public. Monitoring and supervisory authorities in the field of economic affairs often tend to present the latter argument.

Generally, the increased willingness of authorities to publish information online or to otherwise grant access is nonetheless one positive knock-on effect of the right of access to information. Pursuant to the Freedom of Information Act[48] the authorities are supposed to keep directories identifying the available information resources and the purposes of the collected information. Such directories as well as organisational and filing plans without any reference to personal data and other appropriate information are to be made generally accessible. This statutory and administrative approach results in the reduction of applications for access to the respective information and the containment of additional administrative expenditure.

Although up to now apparently not observed, an adverse knock-on effect might be that especially in politically sensitive areas less information could be recorded and retained in order to preclude a subsequent obligation to grant access to such information (at least in the absence of detailed provisions on record keeping and management of files).

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.

The Federal Administrative Court has not had to decide yet the question of which kind of cases are to be determined as abuse or misuse of the right to information. The Freedom of Information Act does not include an abuse clause. According to the explanatory memorandum of the law, the unwritten general principle of administrative law applies

[48] See Art. 11 of the Freedom of Information Act.

that querulous applications do not have to be handled.[49] The practical application of this principle, though, may be difficult. It should be interpreted restrictively in view of the purpose of the law.

Regardless of the applicant's intention, an unreasonable administrative expenditure might lead to a limitation of access to information. Therefore this reason for rejection only serves to prevent misuse or abuse if its requirements are met independently from the questionable intention.

The Freedom of Information Act specifies[50] that fees and expenses are charged for individually attributable public services. Only the furnishing of basic items of information is free of charge. Fees shall though be calculated – with due regard to the administrative expenditure involved – such as to ensure that access to information can be claimed effectively. An abuse fee is not provided for. Therefore misuse and abuse can hardly be prevented by means of charging fees. The Ordinance on Fees and Expenses under the Freedom of Information Act ("Informationsgebührenverordnung – IFGGebV") of 2nd January 2006[51] contains a charging framework of 15 to 500 Euros for the provision of information and documents. Even excessive requests for information cannot be charged with higher fees. Additional expenses can only be imposed for the production of photocopies, printouts and other quantifiable expenses.

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.

a) Art. 7 Subsection (e) Directive 95/46/EC

Processing of personal data is allowed – inter alia –, if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (Art. 7 Subsection (e) Directive 95/46/EC). This is not an exception for security institutions in a broader sense, but a general rule for data processing especially in the public sector. In the public sector an „unambiguous consent" (Art. 7 (a) Directive 95/46/EC) is also recognized as a legitimation for data processing, but in practice it is not as important as in the private sector.

General rules for data processing allow the collection, processing and use of personal data only if permitted or prescribed by this act or any other legal provision or if the data

[49] In German: BT-Drs. 15/4493, p. 16 (http://dip.bundestag.de/extrakt/15/019/15019585.html).
[50] See Art. 10 of the Freedom of Information Act.
[51] In German: BGBl I 2006, p. 6 (http://www.bgbl.de/banzxaver/bgbl/start.xav?start=//*[@attr_id=%27bgbl106s1815.pdf%27]#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl106s0006.pdf%27]__1426785597880).

subject has consented.[52] In Germany, data protection is governed by numerous laws and regulations which can be classified into the federal legislation (The Federal Data Protection Act; federal data protection regulations governing specific areas) and state legislation (data protection acts of the states, state data protection regulations governing specific areas). Data processing has to be permitted and determined by general or specific legal provisions; the data subject's right of access and to correction, erasure or blocking data[53] must be specified. In determining which law or regulation is applicable it is to be considered whether data are processed by public or private entities, furthermore, whether data are processed by a federal or state agency and finally whether data processing by a specific agency and/or a specific purpose of data processing is governed by a special regulation, as those special regulations take precedence over general legislation.

In serving public interest public administration usually involves processing of personal data. Therefore, laws and legal provisions regulating an agency`s specific competence very often also allow processing of those personal data necessary to fulfil the agency´s task. By general rule an institution shall be allowed to collect personal data if knowledge thereof is needed to perform its duties;[54] the storage, modification or use of personal data shall be admissible if it is necessary for the performance of the duties of the controller of the filing system and if it serves the purposes for which the data were collected.[55]

Data processing of security, law enforcement and defense institutions is regulated by special laws. On federal level, the German Code of Criminal Procedure regulates extensively the collection of information (including personal data) by seizure, interception of telecommunication, computer-assisted inquiries , use of technical devices, use of undercover investigators and searches.[56] Further provisions concern handling of personal data in this context, for example, provisions on data files.[57] The Federal Police Act, the Federal Criminal Police Office Act and the state laws on police and public order provide for similar provisions concerning data processing for protection against threats to public order and safety as well as for preventing crime. They allow – under certain conditions – a hidden collection of personal data without the consent and information of the data subject and restrain the data subject's right of access to maintain the confidentiality of sensitive information.

Data processing of German intelligence and secret services (the Federal Intelligence Service [responsible for the collection and evaluation of foreign information concerning the security and other interests of the Federal Republic of Germany]; the Military

---

52 Art. 4 Subsection (1) Federal Data Protection Code.

53 For example Art. 19, 19a. 20 und 21 Federal Data Protection Code.

54 Art. 12 Subsection (1) Federal Data Protection Code.

55 Art. 14 Subsection (1) Federal Data Protection Code.

56 Chapter VIII (Section 94 till Section 111p) Code of Criminal Procedure.

57 Section 483 till Section 491 Code of Criminal Procedure.

Protection Intelligence Agency [responsible for intelligence activities protecting the armed forces and other agencies of the Ministry of Defense]; the Federal Agency for the Protection of the Constitution [that is the domestic intelligence service]) is regulated by specific statutes founding the agency, specifying its tasks and duties and regulating its competence. For example, these statutes contain provisions on the collection of information by special technical means without the data subject or the general public being informed or the competence to compel disclosure of telecommunication data or duties of public agencies to deliver information.The basic structure of these statutes is similar. Their first provisions describe the general task of the agency (for example: providing for security and protecting national interests; collecting and evaluation of information and personal data concerning efforts against national security, on foreign secret service activities or other endangerments to the armed forces; gathering information for security checks of staff, being deployed in „sensitive" areas of the public or private sector), its competence and its cooperation with other security agencies and/or the public and private sector. Other provisions regulate the collection and processing of information and personal data. They allow the collection and processing of information and personal data, if and insofar as the agency concerned needs information to fulfil its task. In particular, these provisions allow and regulate the use of hidden and/or technical methods of collecting information, determine the conditions that must be fit to use those „specific methods" , set up the procedural rules, that must by observed, and regulate, whether or under which circumstances an internal controlling institution, the data subject and/or the general public must be informed.

According to the German Constitution[58] the laws may provide that people affected by hidden control of correspondence, post and telecommunication do not necessarily need to be informed of their surveillance and that recourse to the courts may be replaced by recourse to agencies or auxiliary agencies appointed by the legislature, if constraints to the freedom of correspondence, post and telecommunication aim to protect the free democratic basic order or the existence or security of the federation or a federal state.

b) Art. 8 (4) Directive 95/46/EC

Art. 8 (2) Directive 95/46/EC enumerates personal data which may be of specific importance for the data subject, and prohibits data processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life („special types of personal data"). Art. 8 (2) Directive 95/46/EC includes several exemptions of the prohibition of Subsection (2). Subsection (4) allows further exemptions by national law for reasons of substantial public interest, if there are suitable safeguards.

[58] Art. 10 Subsection (2) Basic Law for the Federal Republic of Germany.

The underlying concept of specific „sensitive data“ is outdated; the relevance of information for personality depends on the context, in which the information is used, not on the information itself. Nevertheless, Art. 8 (1) Directive 95/46/EC has to be obeyed and was transferred into national law.[59] The Federal Data Protection Act allows the collection and processing of special types of personal data beyond the cases enumerated in Art. 8 (2) Directive 95/46/EC inter alia in so far as such collection is necessary in order to avert a substantial threat to public safety, to avert substantial detriment to common weal, to protect substantial interests of common weal, to enable a public body of the federation to perform its duties for compelling reasons of defense or to discharge supranational or international duties in the field of crisis management or conflict prevention or for humanitarian measures.[60] The storage, modification or use of special types of personal data for other purposes shall be permissible only (inter alia) if the requirements which would permit collection in accordance with Section 13 (2), Nos. 1 to 6 or No. 9 are met, hence in all case where intelligence or secret service tasks and interests are concerned. Therefore, special laws and provisions concerning security/defense agencies do not provide for explicit regulations on the collection and processing of special types of personal data.

c) Art. 8 (5) Directive 95/46/EC

Due to Art. 8 (5) Directive 95/46/EC processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority. National provisions may make exemptions, if suitable specific safeguards are provided, subject to derogations which may granted by the Member State under national provisions providing suitable specific safeguards.

Processing of data relating to offences, criminal convictions or security measures is concentrated at public authorities (police, public prosecution departments, criminal courts, public penal facilities). The record-keeping authority of the complete register of criminal convictions is a public, official agency.[61] Personal data relating to administrative sanctions or judgements in civil cases are regularly processed by (and not only under the control) of official authorities also.

Of course in many cases personal data relating to offences, criminal convictions or security measures are not exclusively under the control of official agencies. Some examples: In criminal trials defense lawyers have access to personal data, in the case of public interest media may reveal information, insurance companies may collect and process such data in order to prevent fraud or data may be used by scientific institutions for purposes of scientific research on crime. Official authorities may even be entitled by

[59] Art 3 Subsection (3) Federal Data Protection Act.

[60] Art. 13 Subsection (2) Nos. 5, 6 and 9 Federal Data Protection Act.

[61] See Art. 1 Subsection (1) Federal Central Register Act (Federal Office of Justice [Bundesamt für Justiz]).

law to inform private institutions on offences, criminal convictions or security measures. Processing these data underlies an intensive control of proportionality, but there are no specific rules and there are no specific safeguards, specific controlling standards or other specific means of securing control by official authorities. The collection, processing and use of data is, however, subject to the general monitoring, which is supposed to be sufficient.

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 some complaints that the complexity of the German legislation on data protection is detrimental to its effectiveness. That might be true in some areas of general data processing by „regular" public agencies. In the sector of security, law enforcement and defense institutions the data protection level is insufficient. One of the main problems is to control data processing in a situation of mass data processing („big data"). Especially the competence of intelligence and secret services to surveil telecommunication , the possibility of access to the masses of data stored by private companies and the considerably improved technical facilities for large-scale processing of personal data („data mining") are problems which deserve to be solved.

Another problem is the international, cross border cooperation of intelligence and security agencies. Exchange of personal data and information for security purposes may be important and justified. However, an uncontrolled and mostly uncontrollable data exchange without a fair and clear evaluation of the benefits will undermine restrictions of national laws and regulations. Telecommunication and internet are technically no longer bounded in national areas, so protection of the telecommunication secret cannot be guaranteed by national agencies/provisions alone.