GUTACHTEN

ÜBER ORGANISATIONSFORM UND ZUSTÄNDIGKEITEN

DER DATENSCHUTZBEHÖRDEN IN AUSGEWÄHLTEN STAATEN

(DEUTSCHLAND, FRANKREICH, ITALIEN, NIEDERLANDEN, POLEN, SCHWEDEN,

DAS VEREINIGTE KÖNIGREICH, FINNLAND, SLOWENIEN UND SPANIEN)

Avis 12-224

Lausanne, den 25. Juli 2013
Class. ISDC: CA/D, E, F, I, NL, PL, S, SF, SLOV, UK, 65.1

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

Das vorgelegte Gutachten bietet einen vergleichenden Überblick über Organisationsformen der nationalen Datenschutzbehörden, über die innerstaatlichen Verfahren für die Umsetzung der Datenschutzvorschriften und über die Rechtsbehelfe in den zehn ausgewählten Staaten zur Sanktionierung und zum materiellen Ausgleich von Verstössen gegen den Datenschutzvorschriften, und analysiert die Rolle der Datenschutzbehörden in Bezug auf das Grundrecht des Datenschutzes allgemein. Es untersucht insbesondere die Unabhängigkeit, Effizienz und das Funktionieren der Kontrollstellen.

Alle untersuchten Rechtsordnungen haben einen Rechtsrahmen erarbeitet, durch den die Vorgaben des Datenschutzes umgesetzt werden.

In allen untersuchten Staaten können Einzelpersonen eine Klage im Zusammenhang mit einem spezifischen Verstoss oder eine allgemeinere Beschwerde vor der Datenschutzbehörde erheben, um auf einen Verstoss hinzuweisen. Ein wesentlicher Grundsatz der Rechtsstaatlichkeit ist das ebenfalls in allen analysierten Staaten anerkannte Recht, vor ordentlichen Gerichten ein Verfahren anzustrengen, um eine gerichtliche Entscheidung über den Rechtsstreit zu erlangen. Dies kann gewöhnlich auch im Wege vereinfachter Verfahren geschehen. In einigen Staaten (z.B. Frankreich oder Polen) haben betroffene Personen die Option, Rechtsstreitigkeiten entweder vor Gericht vorzutragen oder entsprechende Beschwerden bei den Datenschutzbehörden einzureichen, die in einem quasi-gerichtlichen Verfahren möglicherweise einen rasch wirksamen und kostengünstigen Rechtsbehelf bieten können.

Die Datenschutzbehörden müssen über die erforderlichen Ressourcen verfügen und mit entsprechenden Befugnissen sowie der gebotenen Unabhängigkeit ausgestattet sein, um zur wirksamen Durchsetzung des Datenschutzsystems beitragen zu können. Deswegen wird im Gutachten eingehend analysiert, mit welchen Untersuchungs-, Einwirkungs-, Beratungs- und Befassungsbefugnissen und in welchem Umfang die Datenschutzbehörden ausgestattet sind.

Der Schutz personenbezogener Daten wird in verschiedenen europäischen und internationalen Verträgen als Grundrecht anerkannt und in der Rechtsprechung internationaler und regionaler Gerichte ausgelegt. Das Grundrecht auf den Schutz personenbezogener Daten wird auch auf globaler Ebene in verschiedenen unter der Federführung der Vereinten Nationen erlassenen Menschenrechtsinstrumenten anerkannt, überwiegend als Erweiterung des Rechts auf Privatsphäre. Auf regionaler Ebene beruht der Standard für den Schutz personenbezogener Daten auf mehreren Übereinkommen, die besonders im Rahmen des Europarats angenommen wurden. Die meisten dieser Instrumente wurden von allen EU-Mitgliedstaaten ratifiziert und teilweise in den einzelstaatlichen Rechtssystemen als Verfassungsnormen eingeführt. Durch den Auftraggeber für das Gutachten bestimmte Staaten sind alle Mitgliedstaaten der Europäischen Union. In diesem Zusammenhang muss darauf hingewiesen werden, dass die Organisationsform und Zuständigkeiten der Datenschutzbehörden in allen Mitgliedsstaaten vor allem auf der Umsetzung der EU-Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (im Folgenden die „Datenschutzrichtlinie“) basieren. Die Datenschutzbehörden sind damit ebenfalls ein wichtiges Element der EU-Grundrechte-Architektur; der EU kommt nämlich eine Vorreiterrolle bei der Behandlung des Datenschutzes als Grundrecht zu, und die EU hat in vielen Mitgliedstaaten entscheidend zur Entwicklung von Datenschutzsystemen beigetragen. Der Datenschutz ist auch eines der entscheidenden Politikfelder im Bereich der Grundrechte, in denen die EU die Zuständigkeit zur Erlassung von Rechtsvorschriften besitzt. Bislang hat die EU den Datenschutz auch als Instrument der Harmonisierung des

Binnenmarkts betrachtet; dieses Instrument sollte den Schutz eines Grundrechts innerhalb der Gemeinschaft unterstützen.

Die Mitgliedstaaten der EU sind verpflichtet die Datenschutzrichtlinie wirksam durchzusetzen. Die Agentur der Europäischen Union für Grundrechte[1] hat in diesem Zusammenhang eine Analyse der Rolle der Datenschutzbehörden[2] in Bezug auf das Grundrecht des Datenschutzes und der Bewertung der Effizienz und des Funktionierens und der Unabhängigkeit der Datenschutzbehörden in der EU durchgeführt. Das Ergebnis dieser Analyse zeigt, dass eine ordnungsmässige EU-weite umfassende Gesamtbeurteilung der problematischen Bereiche insbesondere mangels an systematischer und statistischer Daten kaum möglich scheint. Dies musste auch in der vorliegenden Studie festgestellt werden.[3]

---

1 Agentur der Europäische Union für Grundrechte http://fra.europa.eu/de

2 Datenschutz in der die Rolle der nationalen Datenschutzbehörden Stärkung der Grundrechte-Architektur in der EU – Teil II;
http://fra.europa.eu/sites/default/files/tk3109265dec_de_web.pdf

3 „Die Beurteilung der Einhaltung der Standards ist jedoch verhältnismässig problematisch. In vielen Fällen können die nationalen Datenschutzbehörden aus Personalmangel keine systematische und statistische Darstellung der Situation vor Ort liefern. Aber auch wenn diese statistischen Daten vorliegen, sind sie nicht immer kohärent und ausreichend, um die Situation ordnungsgemäss darstellen zu können. Es war daher unmöglich, zu einer EU-weiten und umfassenden Gesamtbeurteilung des Grades der Einhaltung der Standards und/oder der in den Gesetzen und in der Praxis problematischen Bereiche zu gelangen.“, Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden Stärkung der Grundrechte-Architektur in der EU – Teil II, 2012; S. 31 http://fra.europa.eu/sites/default/files/tk3109265dec_de_web.pdf

I. SACHVERHALT

Das Datenschutzgesetz (DSG) ist unter der Federführung des Bundesamts für Justiz (BJ) evaluiert worden. In Bezug auf den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geht aus dem Evaluationsbericht des Bundesrates vom 9. Dezember 2012 hervor, dass die Kompetenzen des EDÖB im internationalen Vergleich nicht besonders stark ausgestaltet sind (BBl 2012 345), dieser im Rahmen seiner Möglichkeiten aber wirksam vor missbräuchlichen Datenbearbeitungen schützt und die Schutzwirkung des Datenschutzgesetzes erhöht. Die Bedeutung des EDÖB dürfte inskünftig noch zunehmen, weil die Nutzerinnen und Nutzer der neuen Kommunikationstechnologien ihre Persönlichkeit zwar schützen möchten, aber teilweise achtlos und überfordert sind (BBl 2012 348). Die Wirkungsmöglichkeiten des EDÖB stossen indes bereits heute in verschiedener Hinsicht an ihre Grenzen:

Der EDÖB kann seine Aufsicht nur noch erschwert wahrnehmen, weil die Datenbearbeitungen häufiger, unübersichtlicher und internationalisierter geworden sind (BBl 2012 341 f. u. 343, 344). Die Wahrnehmbarkeit von Missbräuchen und der Zugriff auf die Bearbeitenden werden dadurch erschwert und damit auch der Selbstschutz der Betroffenen und die Kontrolle durch den EDÖB (BBl 2012 349). Es gibt ausserdem Hinweise, dass die Pflicht zur Registrierung von Datensammlungen und zur Erstellung von Bearbeitungsreglementen ungenügend durchgesetzt wird, die damit verfolgten Ziele (Transparenz für die Bevölkerung, Sensibilisierung der Datenbearbeitenden) somit nur teilweise erreicht werden dürften (BBl 2012 344). Die mit der Evaluation betrauten Forscher empfehlen eine Stärkung der Aufsichtskompetenzen des EDÖB, etwa mittels einer Ausdehnung seiner Sanktionsmöglichkeiten und seiner Befugnisse bei der Informationsbeschaffung sowie über die Erhöhung seiner Ressourcen (BBl 2012 346). Der Bundesrat lässt deshalb prüfen, ob die Aufsichtsmechanismen des EDÖB gestärkt werden sollten und ob die Unabhängigkeit des EDÖB noch verstärkt werden sollte (BBl 2012 350).

Aufgrund der Ergebnisse der Evaluation ist der Bundesrat der Auffassung, es sei zu prüfen, ob die Datenschutzgesetzgebung anzupassen sei, um den rasanten technologischen und gesellschaftlichen Entwicklungen Rechnung zu tragen. Der Bundesrat werde deshalb unter Berücksichtigung der Ergebnisse der Evaluation, der im Bereich Datenschutz gegenwärtig laufenden Entwicklungen in der Europäischen Union und beim Europarat sowie aller konkret betroffenen Interessen vertieft prüfen, welche gesetzgeberischen Massnahmen getroffen werden können (BBl 2012 336).

Der Bundesrat hat das EJPD mit Beschluss vom 9. Dezember 2011 beauftragt, zu prüfen, welche gesetzgeberischen Massnahmen getroffen werden können, um die Wirksamkeit des DSG zu erhöhen, und ihm bis spätestens Ende 2014 Vorschläge zum weiteren Vorgehen zu unterbreiten. Dabei seien namentlich die Ergebnisse der Evaluation und die Entwicklungen in der EU und im Europarat zu berücksichtigen.

Zur Schaffung von Entscheidgrundlagen für einen Teilaspekt dieses Auftrags gibt das BJ eine Studie in Auftrag.

Zur Berücksichtigung der verschiedenen Systeme soll die Studie die Datenschutzbehörden von Deutschland, Frankreich, Italien, den Niederlanden, Polen, Schweden und des Vereinigten Königreichs untersuchen.

Die Abklärungen zum ausländischen Recht werden vom Schweizerischen Institut für Rechtsvergleichung (SIR) vorgenommen.

II. FRAGESTELLUNG

1. Allgemeine Ausgestaltung der Behörde

- Was sind die verschiedenen Organisationsformen (Kommission, Verantwortliche Person – z.B. Datenschutzberaterin oder Preisüberwacher – Verantwortlicher mit Beirat, u.a.m.)?
- Wie gross sind die Kommissionen, Beiräte etc.? Wie sind sie mit Mitarbeitenden ausgestattet?
- Was ist die Stellung der Behörde (Teil der Verwaltungshierarchie, unabhängige Kommission)?
- Was sind die Kompetenzen des Präsidenten bei Kollegialbehörden? Haben einzelne Mitglieder (z.B. der Präsident) besondere Kompetenzen?
- Komplexität: Gibt es Behörden auf nationaler, regionaler, lokaler Ebene? Wie sind die Zuständigkeiten für die verschiedenen Aufgaben koordiniert? Wie diejenigen für Gesetzgebung/Vollzug?
- Wieso wurde die Organisationsform gewählt? Wurde diese von Anfang an so gewählt oder im Laufe der Zeit entwickelt? Wenn ja, aus welchen Gründen?
- Was für Vorkehrungen bestehen, um die Unabhängigkeit der Behörde zu sichern und Interessenkonflikte zu vermeiden? Welche Elemente stärken die Unabhängigkeit (z.B. Organisationsform, Anzahl Mitglieder)?
- Wird die Behörde von den wichtigsten Anspruchsgemeinschaften als neutral beurteilt, oder vertritt sie in ihren Augen z.B. Betroffene oder politische Interessen?
- Was sind die Vorteile und Nachteile der Organisation? Welches andere Modell wird gegebenenfalls von den Mitgliedern der Behörde und den wichtigsten Anspruchsgemeinschaften bevorzugt?

2. Wahl und Stellung der Behördenmitglieder

- Von wem werden die Behördenmitglieder (z.B. die Datenschutzberaterin) gewählt oder angestellt (von der Regierung, dem Parlament)? Was sind die Kriterien (z.B. Repräsentanten von Anspruchsgemeinschaften oder Parteien, fachliche Qualitäten)?
- Was sind die persönlichen und fachlichen Anforderungen? Was sind die Bedingungen bezüglich Parteizugehörigkeit, Verwaltungsratsmandaten und andere Interessenbindungen? Was für Unvereinbarkeiten bestehen?
- Sind Nebenbeschäftigungen zulässig? Gibt es Einschränkungen? Wie wird sie beurteilt (z.B. als Bereicherung für die Behörde, oder als Quelle von Interessenkonflikten)?
- Wie verbreitet ist Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe? Was sind die Gründe für Voll- oder Teilzeitlösungen?
- Wie lange ist die Amtsdauer? Ist Wiederwahl möglich? Wie oft?
- Wie ist das Arbeitsverhältnis ausgestaltet (z.B. Magistrat, Beamtenstatus oder Angestelltenverhältnis, Kündigungsschutz, Beurteilungssystem)?
- Sind die Behörde und deren Mitglieder und Mitarbeitenden unabhängig von Weisungen und Interessenbindungen? Bestehen Abhängigkeitsverhältnisse?

3. Ressourcen

- Wer hat die Budgethoheit für die Behörde (Budgetgenehmigung durch das Parlament, die Regierung)?
- Was sind die Einnahmequellen der Behörde, kann sie z.B. Gebühren erheben?
- Verfügt die Behörde über ein eigenes Budget? Ist dieses adäquat für die Erfüllung der Aufgaben?

- Wie gross ist das Budget im Quervergleich mit den vergleichbaren Behörden?

4. Aufgabenerfüllung

- Wie zugänglich ist die Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)? Reagiert sie eher reaktiv oder präventiv? Wie berechenbar ist sie? Sind ihre Aussagen verbindlich?
- Wie ist die Akzeptanz und das Ansehen der Behörde in den interessierten Kreisen (Behörden, Verwaltung, Wirtschaft, Datenschutzvereinigungen, Experten), wie wird ihre Legitimation beurteilt? Wie wird ihr Wirken und ihre Effizienz beurteilt? Besteht z.B. ein Konflikt-Aufsichts-Beratung? Was für Lücken werden bemängelt, was für Verbesserungsvorschläge vorgebracht?
- Wo liegt der Schwerpunkt der Tätigkeit? Wie werden die Ressourcen für die verschiedenen Aufgaben eingesetzt? Wie sieht die Arbeitsteilung aus (Präsidentin – Behördenmitglieder – Mitarbeitende)?
- Was sind die Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen (Empfehlung, Verfügung, Mediation, Klage vor Gericht, etc.)? Wie werden diese genutzt (absolut und im Vergleich zueinander)? Mit welchem Ergebnis bzw. Erfolg?
- In einigen Ländern (z.B. Deutschland oder Vereinigtes Königreich) ist – wie bei uns der EDÖB – die gleiche Behörde für den Datenschutz und das Öffentlichkeitsprinzip zuständig. Wie wirkt sich das auf die Effizienz bei der Durchsetzung des Datenschutzes aus? Ist diese Doppelrolle von Vorteil oder von Nachteil?
- Besteht ein Zusammenhang zwischen einer bestimmten Organisationform und den Aufgaben, die die Behörde erfüllt?

5. Schlussbeurteilung

Gesamtwürdigung der Forschungsergebnisse in Bezug auf die in der Evaluation georteten Schwächen mit Aussagen zu möglichen Lösungsansätzen.

III. ANALYSE

A. Tabellarische vergleichende Übersicht

1. Allgemeine Ausgestaltung der Behörde

	Stellung der Behörde (Unabhängig: U; unter dem Justizministerium: J; Unter dem Parlament: P; Unter der Exekutive: E; andere)	**Organisationsform (Kommission, Berater, Berater mit Beirat: andere)**	**Grösse**	**Bestehen mehrere oder einer einzelnen Behörde**
Deutschland	U (aber organisatorisch mit dem Innenministerium verbunden)	Berater, Leitender Beamter, 9 Fachreferate	ca. 90 MA	eine Behörde; auf Länderebene eigene Behörden
Frankreich	U	Kommission	17 Mitglieder + ca.160 « agents » (durch den Präsidenten rekrutiert)	Eine Behörde
Italien	U	Kommission (Garante) + Administratifvorgang mit Generalsekretariat	4 Mitglieder + 125 MA (Einheiten)	Eine Behörde
Niederland	U	Kommission + Sekretariat	3 Mitglieder + Sekretariat mit ca. 80 MA	Eine Behörde
Polen	U	Berater (Inspektor)	Ca. 129 MA	Eine Behörde
Schweden	J-U: Autonomous Government agency which falls under / organized under the Ministry of justice	Verwaltungsbehörde	Ca. 40 MA	Eine Behörde
Vereinigtes Königreich	J-U: Non-departmental public body sponsored by the Ministry of Justice	Berater (Commissioner), unterstützt durch eine Kommission	350 MA	Eine Behörde
Finnland	The **Office of the Data Protection Ombudsman ("ODPO")**: operates in connection with the Ministry of Justice: J. The **Data Protection Board ("DPB"):** affiliated to the Ministry of Justice: J.	The **ODPO** is an independent authority (In Swedish: chefsämbetsverk) operating in connection with the Ministry of Justice. The **DPB** is a board affiliated to the Ministry of Justice.	**ODPO**: 20 staff**.** The **DPB**: 7 members and a secretary.	Two authorities: the **ODPO** and the **DPB.**
Slowenien	U	Berater (Information Commissioner)	33 MA	Eine Behörde

Spanien	U-J : L'Agence espagnole de protection de données (AEPD) jouit d'un statut indépendant. L'AEPD est lié au Ministère de la justice.	L'AEPD est une enti*t*é de droit public, dotée de personnalité juridique propre et de capacité pour agir indépendamment, tant dans les domaines publique que privée. Elle est en liaison avec le Ministère de la justice.	L'AEPD emploie 154 fonctionnaires (la dotation étant de 157), 2 employés (la dotation étant de 7) et 1 haut fonctionnaire. Parmi ceux-ci, 91 sont des femmes et 69 des hommes.	L'AEPD agit au niveau national. Il existe des autorités régionales et locales agissant dans certaines des Communautés autonomes. Ces dernières doivent respecter les attributions de compétences attribuées aux régions par la Constitution espagnole.

2. Behördenmitglieder und Mitarbeitende

	Zuständiges Organ für Wahl / Ernennung	Persönliche und fachliche Anforderungen	Zulässigkeit der Nebenbeschäftigungen	Länge der Amtsdauer, Wiederwahlmöglichkeit	Ausgestaltung des Arbeitsverhältnisses
Deutschland	Wahl durch den Bundestag (Parlament) auf Vorschlag der Bundesregierun; Ernennung durch den Bundespräsidenten (der keine Auswahlbefugnis hat)	Mindestalter 35 Jahre sowie allgemeine Voraussetzungen zur Bekleidung eines öffentlichen Amtes	keine Nebenbeschäftigungen zugelassen	5 Jahre, einmalige Wiederwahl möglich	BfDI: öffentlich-rechtliches Dienstverhältnis eigener Art; nachgeordnete Mitarbeiter: Beamte des Bundeministeriums des Innern
Frankreich	12 membres sont élus par les assemblées ou juridictions auxquelles ils appartiennent (Assemblée Nationale, Sénat, Cour des comptes, Cour de cassation, Conseil d'Etat, le Conseil économique et social), 3 personnalités sont nommées par décret et deux autres (une par le Président de l'Assemblée Nationale, l'autre par le Président du Sénat). Les agents contractuels sont désignés par le Président de la CNIL.	Indépendance, compétences juridiques et/ou en informatique.	Art 14 I de la loi du 6 janvier 1978 : « la qualité de membre de la commission est incompatible avec celle de membre du Gouvernement » Art. 14 III : « Tout membre de la commission doit informer le président des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale. Ces informations, ainsi que celles concernant le président, sont tenues à la disposition des membres de la commission. »	cinq ans renouvelable une fois, à l'exception des membres issus du Conseil économique et social, de l'Assemblée Nationale et du Sénat qui sont élus pour une durée égale à celle de leur mandat dans leurs institutions respectives	Les agents de la CNIL sont recrutés librement par le Président de la CNIL et ont le statut d'agent contractuel de l'Etat. Ils sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 ainsi qu'au décret du 20 octobre 2005.
Italien	Parlamento	Indipendenza, riconosciuta competenza nelle materie del diritto o dell'informatica	I membri del Garante, per tutta la durata dell'incarico, non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive	Mandato di sette anni non rinnovabile	I membri del Garante sono eletti. Il trattamento giuridico ed economico del personale di ruolo è disciplinato dal Regolamento del Garante n. 2/2000

Niederland	The government appoints the chairperson, the members, the advisory board and the secretariat.	No particular requirement though the chairperson must meet the requirement as for Cantonal Judges.	Only with permission of the Minister.	Yes, chairperson for 6 years and members for 4 years. Both appointments can be renewed. Members of advisory board for 4 years with maximum of 2 renewals.	Civil servants.
Polen	The Inspector General for Personal Data Protection and his Deputy are elected by the Parliament	Particular requirements: Polish citizen permanently residing within the territory of the Republic of Poland, must be known for outstanding moral principles, must hold a degree in law and have a proper professional experience and no criminal record. He/she must not hold another position except as a professor of a higher education institution nor perform any other professional duties. She/he may not be a member of any political party or any trade union, or be involved in any public activity which is not consistent with the integrity of the Inspector General's post	Only position for a professor of a higher education institution accepted.	The term lasts 4 years may be held for not more than two terms.	Position of an elected officer by the Parliament, and the employees are civil servants.
Schweden	The government appoints the Director-General and the Advisory Council, the rest of the staff are employed by the Board itself.	No particular requirements, only objective factors such as merit and competence	Yes, as long as it does not undermine the confidence in his or any other employee's impartiality or may harm the reputation of the Data Inspection Board.	The Director-General can be appointed for a limited renewable period or a non limited period, other staff non limited period, members of the Advisory Council for a limited period.	The Director-General is employed as "staff in a leading position" and the employees are civil servants (statliga tjänstemän), the members of the Advisory Council are elected and employed for this particular capacity (insynsrådledamot).

Vereinigtes Königreich	Officially appointed by the Queen only on recommendation of Government Minister and endorsement by Parliamentary Committee.	None in particular; appointed on merit on the basis of fair and open competition	No specific provisions on secondary employment, but senior posts are full time and require declaration of other interests in formal register	No longer possibility of re-election; appointment is for fixed term of 7 years	The Information Commissioner is a 'corporation sole' – akin to a Bishop – and is not classified as a civil servant. Staff of the Commission are employees of a public body and are expressly not employed as civil servants.
Finnland	The Data Protection Ombudsman ("DPO") and the members of the DPB are appointed by the government. The deputy to the DPO is appointed by the Ministry of Justice. Other staff in the office are employed by the DPO.	The DPO: LL.M., good knowledge of data protection matters, leadership skills. Similar requirements for DPO's deputy. Other staff: University degree or other suitable education. DPB members: familiar with data register activity, LL.M for the chair and two other members.	The staff at the ODPO can pursue a secondary activity/employment provided that inter alia it is not pursued during the regular work and as long as it does not undermine the confidence in his or any other employee's impartiality. No regulations regarding the DPB members.	The DPO: renewable period of maximum 5 years at the time. The members of the DPB: renewable period of 3 years at the time.	The DPO with assistance of his deputy (in Swedish: byråchef) is running the ODPO. Remaining staff are civil servants. The members of the DPB are appointed as board members (in Swedish: Datasekretessnämndens medlemmar).
Slowenien	Information Commissioner is appointed by the National Assembly on recommendation of the president	Particular requirements: - be a citizen of the Republic of Slovenia; - hold a university degree; - have at least five years of working experience; - must not have been convicted by a final decision of a criminal offence punishable by an unconditional punishment of deprivation of liberty	Position of the Information Commissioner is considered as full time job. All employees' posts are rated as full time roles.	Information Commissioner is appointed for a five year term and can be reappointed once.	Position of an appointed state officer by the Parliament, and the employees are civil servants.
Spanien	Le Directeur de l'AEPD Il est nommé par décret royal parmi les membres du conseil consultatif, pour une période de quatre ans. Les membres du Conseil consultatif de l'AEPD sont nommés par le gouvernement sur proposition préalable que diverses entités	Le Directeur est choisi parmi les membres du Conseil consultatif.	La loi espagnole sur les incompatibilités dans le service (Ley 9/1991, de 22 de marzo RCL\1991\799), s'applique aux hautes charges de l'état. Nous n'avons pas trouvé d'indices sur la possibilité de faire des activités accessoires par des employés de rang plus bas.	Le Directeur de l'AEPD est nommé par décret royal parmi les membres du conseil consultatif, pour une période de quatre ans.	Le Directeur de l'AEPD agissant étant qu' „haute charge de l'état" dirige l'agence. Il consulte le comité consultatif.

	publiques ont fait au Ministère de la justice. Le Conseil consultatif de l'AEPD est composé de la façon suivante : a. le Congrès des députés désigne un membre (un député), b. le Sénat désigne un membre (un sénateur), c. le Ministre de la justice désigne un membre appartenant à l'administration de l'État, d. les Communautés autonomes désignent un membre par décision prise à la majorité, e. la Fédération espagnole des municipalités et des provinces désigne un membre de l'administration locale, f. l'Académie royale d'histoire désigne un membre appartenant à celle-ci, g. le Conseil des universités désigne un membre expert dans le traitement de données automatisées, h. le Conseil de consommateurs et usagers désigne un membre, i. le Conseil supérieur de Chambres de commerce, de l'industrie et de la navigation désigne un membre. Les membres choisis par ces entités sont présentés au				

	gouvernement par le Ministère de la justice. La durée de leur mandat est de quatre ans				

3. Unabhängigkeit und Umgang mit Interessenkonflikten

	Unabhängigkeit der Behörde/Behördenmitglieder	Weisungen von Aussen	Neutralität der Behörde
Deutschland	unproblematisch bezüglich des BfDI selbst; problematischer hinsichtlich der nachgeordneten Mitglieder, die formell Bedienstete des Innenministeriums sind und nach ihrer Tätigkeit für den BfDI möglicherweise dort weiter aufsteigen möchten (vgl. 2.2)	keine	keine gegenteiligen Äusserungen/Meinungen bekannt
Frankreich	Art. 11 alinéa 1 de la loi du 6 janvier 1978 : la CNIL est une « autorité administrative indépendante ». Art. 21 alinéa 1 « Dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité ».	Non. La CNIL est toutefois consultée par les autorités publiques, y compris par les juridictions. Elle doit répondre à toute demande d'avis de leur part.	Pas de disposition particulière mais dans son ordonnance de référé rendue le 19 février 2008, le Conseil d'Etat qualifie la CNIL « de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».
Italien	L'indipendenza del Garante è assicurata soprattutto dalle modalità di nomina dei suoi membri	Ridotta	Sufficientemente garantita
Niederland	An independent governing body. Instructions are laid down in a *bestuursreglement* which needs approval from the Minister.	Only the Minister can instruct that a certain subject needs more attention.	Neutral based on their function in an independent governing body.
Polen	Independent, one-person authority	Solely subject to the provisions governed by the Law. No other instruction than in legislation.	Neutral based on their function as an independent body.
Schweden	Autonomous government agency which pursues activity in accordance with legislation and general guidelines from the government. / Director-General is appointed by the government but represents only the agency (not the government), the members of the Advisory Council represent the public (the aim is that the Council provide info to the public about the work of the Agency)	No other instruction than in legislation and general ordinances and guidelines from the government.	The Data Inspection Board is neutral in the sense that it is not controlled nor need it consider instructions/requests originating from particular political interest or other stakeholders.
Vereinigtes Königreich	The Information Commissioner is appointed not as a civil servant but as a 'corporation sole', highlighting in statute (the Data Protection Act 1998) his independence from Government; a Framework Agreement between the Information Commissioner and the Ministry of Justice provides further guidance on the independence of the office. He/she is accountable to Parliament rather than to the Ministry of Justice.	Instructions from outside the Information Commission are confined to limited areas where Ministerial consent is required, principally regarding the spending of public funds.	No specific provisions, but safeguards as to neutrality provided for in appointments process and designated remit of Information Commissioner and Office as independent regulator.

Finnland	The ODPO is an independent authority operating in connection with the Ministry of Justice. Justice and independence are values which are the basis for its activities and position. The DPB is an independent authority affiliated to the Ministry of Justice. There are no explicit provisions laid down in law regarding the independence of the DPO nor the members of the DPB.	Instructions for the DPO and the DPB are laid down in legislation and in government ordinance. There are no instructions from other public or private bodies.	The DPO shall be free from all other activities and posts pursued, thus the DPO shall not represent any partisan interests. There are no rules regarding the neutrality of the members of the DPB. Instructions for these two authorities are laid down in legislation and government ordinance.
Slowenien	Independent, one-person authority appointed by the Parliament. He/she is solely subject to the provisions governed by the Law.	No legal possibility for instructions from outside.	The Institution is considered as neutral (impartial and independent).
Spanien	L'AEPD es tune agence indépendante de droit public.	L'AEPD ne reçoit pas d'instructions d'autres entités.	Il n'y a pas des dispositions destinées spécifiquement à sauvegarder la neutralité, mais la constitution des autorités de l'AEPD ainsi que la façon dont celles-ci sont élues, ainsi que la large indépendance accordé à l'AEPD semblent aller dans le sens de garantir la neutralité. D'une manière générale, l'Espagne prévoit des règles L'Espagne prévoit des règles d'abstention et de récusation des fonctionnaires en raison d'incompatibilités (loi du 17 1958 - RCL\1958\1258 et loi 9/1991, de 22 mars 1991[4].

[4] Ley 9/1991, de 22 de marzo - RCL\1991\799 INCOMPATIBILIDADES. Modifica determinados preceptos de la Ley 25/1983, de 26-12-1983 (RCL□1983\2806 y ApNDL 1975-85, 6586), de incompatibilidades de altos cargos; de la Ley 7/1985, de 2-4-1985 (RCL□1985\799 , 1372 y ApNDL 1975-85, 205), reguladora de las Bases del Régimen Local; de la Ley de Contratos del Estado, texto articulado aprobado por Decreto 8-4-1965 (RCL□1965\771 , 1026 y NDL 7365), y de la Ley 24/1988, de 28-7-1988 (RCL□1988\1644 ; RCL□1989\1149 y 1781), del Mercado de Valores ».

4. Ressourcen

	Budgethoheit	Einnahmequellen der Behörde
Deutschland	„für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung“ wird dem BfDI laut Gesetz im Haushalt des Bundesministeriums des Innern in einem gesonderten Kapitel zur Verfügung gestellt	laut BDSG müssen dem BfDI in einem gesondert ausgewiesenen Teilhaushalt des Bundesministeriums des Innern ausreichende Personal- und Sachmittel zur Erfüllung seiner Aufgaben zugewiesen werden. Gebühren erhebt der BfDI daneben nur in wenigen Fällen.
Frankreich	Autonomie budgétaire (Art.12 de la loi du 6 janvier 1978) mais elle n’a pas d’indépendance financière (le budget de la CNIL dépend du ministère de la Justice).	Il n’y a pas de frais.
Italien	Finanziamento a carico del bilancio dello Stato	Riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge
Niederland	Financed by the Ministry of Security and Justice.	n/a
Polen	State budget adopted by the Parliament	It applies no charges.
Schweden	The overall budget is decided by the government each year; for 2013 the budget is set at about 42 million Swedish crowns.[5]	The Data Inspection Board can charge a fee for goods and services provided to the public with an amount corresponding to 10 per cent of the total costs for the Board’s activity in this regard
Vereinigtes Königreich	Commission is self-funded for data protection activities, but relies on Government funding for freedom of information duties. (see right column).	Data protection activities funded through charging of annual registration fee to data processors (i.e., organisations which process personal data); functions concerning freedom of information funded through ‘grant-in-aid’ direct funding from Ministry of Justice, decided on an annual basis.
Finnland	The budget of the ODPO and for the DPB is decided each year by the government. For 2013 the budget is set to 1,800,000 EURO for the ODPO and 15,000 EURO for the DPB.	The ODPO can charge a fee for its services.
Slowenien	Self-standing accounting item in the Law on State budget adopted by the Parliament	The Institution applies no charges.
Spanien	L’AEPD élabore et approuve chaque année l’avant-projet de son budget annuel et l’adresse au gouvernement pour qu’il soit incorporé au budget général de l’État étant que « item » indépendant.	Les procédures de dénonciation et de consultation des registres sont gratuites.

[5] Regleringsbrev för budgetåret 2013 avseende Datainspektionen p. 3, available at http://www.esv.se/sv/Verktyg--stod/Statsliggaren/Regleringsbrev/?RBID=14572 (2013-03-11).

5. Aufgabenerfüllung

	Zugänglichkeit der Behörde für die Betroffenen	Akzeptanz und Ansehen der Behörde	Handlungsmöglichkeiten / Durchsetzung der Kompetenzen	Schwerpunkt der Einsetzung der Ressourcen
Deutschland	für jedermann zugänglich, der eine Verletzung eigener Rechte durch datenbezogenes Verhalten einer Bundesbehörde geltend macht.	gut	keine direkte Durchsetzungskompetenz, aber hohes Gewicht der Beurteilung durch den BfDI	Beratung und Kritik öffentlicher Stellen; Information der Öffentlichkeit, Berichte; Gutachten zu Gesetzgebungsvorhaben und in Verfahren vor dem Bundesverfassungsgericht
Frankreich	Possibilité d'adresser auprès de la CNIL une plainte, une réclamation ou une pétition (art. 11 2° c) une demande d'accès aux infor-mations contenues dans des fichiers de police ou de gendar-merie, une demande de coordon-nées d'un responsable de fichier	La CNIL a longtemps eu une bonne réputation. Récemment, Il y a eu quelques critiques du fait de l'ampli-fication de ses missions et du manque de moyens.	Pouvoir d'autorisation, de règlementation, de décision, de recommandation, de propo-sitions législatives, d'émission d'avis, d'investigation, de saisir le juge des référés en cas d'atteintes graves ou de dénoncia-tion au parquet, de sanction administrative et pécuniaire.	Aucune information sur les ressources de la CNIL.
Italien	Gli interessati possono rivolgersi al Garante mediante reclamo, segna-lazione, ricorso	Nessuna informazione	Autorizzazioni, provvedimenti su reclami, segnalazioni e ricorsi, pareri, accertamenti, sanzioni	L'organo di vertice, svolge funzioni di indirizzo e controllo sul rispetto delle direttive impartite. L'Ufficio del Garante svolge funzioni di gestione e di attua-zione dei programmi. Il Segretario gene-rale svolge una funzione di raccordo tra la struttura amministrativa e il Garante
Niederland	Data subjects can make a request / file a complaint through www.mijnprivacy.nl	n/a	Supervising compliance with the Dutch Data Protection Act, making recommendations regarding legislation, testing codes of con-duct, testing regulations, notification and preliminary examination, information, exemption from the prohibition to process sensitive data, making recommendations regarding permits for transfers to third countries, international affairs, mediation and handling of complaints, official investi-gation, enforcement, international tasks.	n/a

Polen	Any party may apply for reconsidering its case.	High level of acceptance and confidence	She/he address state authorities, territorial self-government authorities, as well as state and municipal organizational units, private entities performing public tasks, natural and legal persons, organizational units without legal personality and other entities in order to ensure efficient protection of personal data. She/he may also request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relating to personal data protection. The entity receiving the address or request gives an answer in writing to such address or request within 30 days of its receipt. Once a year, the Inspector General submits to the Sejm a report on his/her activities including conclusions with respect to observance of the provisions on personal data protection.	n/a
Schweden	Individuals can make a request / file a complaint at the Data Inspection Board. Such request can lead to an inspection. The Board also provides information in various ways to the public.	High level of acceptance and confidence in comparison to other autonomous government agencies.	The Board can render a decision or an instruction for rectification and can under certain circumstances prohibit (violators being subject to a default fine the controller of personal data to continue processing the personal data in any other manner than by storing them.[6] The Board may at the County Administrative Court apply for the erasure of such personal data that have been processed in an unlawful manner.[7]	One third of the resources are used for inspection duties under the data protection laws, another third is used for the provision of information to the public and to the development of directives and codes of statutes. The rest of the resources are used for all other activities e.g. administrative work.
Vereinigtes Königreich	Direct request may be made by or on behalf of affected person for assessment of data processing compliance	Compared with other regulators, the Information Commissioner's Office is gene-rally accessible to stakeholders, has a good relationship with them and produces extensive and clear and accessible guidance	Power to serve Information Notices seeking further information; Enforcement Notices requiring data controller to take specific steps to rectify contravention; powers of entry and inspection; powers to inspect personal data in overseas information systems; power to impose fines for serious breaches of data protection laws	Broadly, 65% of resources are used for data protection activities, 35% for freedom of information duties and other functions.

6 Article 45 Personal Data Act (1998 :204).

7 Article 47 Personal Data Act (1998 :204).

Finnland	If the controller (e.g. a company or a public authority) of data refuses the request of a data subject (i.e. the person to whom the personal data pertains) of the rectification or erasure of data in its personal data file, the data subject may bring the matter to the attention of the DPO. The ODPO co-operate with data subjects and controllers and other stakeholders, thereby aiming to prevent violation of privacy in advance.	No information is to be found on this matter.	The DPO and the DPB have the right of access (violators being subject to a default fine) to processed personal data. The DPO may order a controller to realise the right of access of the data subject or to rectify an error and report it for prosecution. On the request of the DPO, the DPB may: prohibit processing of personal data; compel the person concerned in certain cases to remedy an instance of unlawful conduct or neglect; revoke a permission granted for the processing of personal data.	Most of the resources are allocated to the ODPO and to its work to influence, in advance, compliance with the legislation regarding the keeping of registers by providing its stakeholders general guidance and consultations.
Slowenien	Individuals can make a request / file a complaint with the Information Commissioner. Such request can lead to an inspection.	High level of acceptance and confidence	The Information Commissioner has the right immediately: 1. to order the elimination of irregularities or deficiencies he detects in the manner and within the interval he himself defines; 2. to order the prohibition of processing of personal data by persons in the public or private sector who have failed to ensure or failed to implement measures and procedures to secure personal data; 3. to order the prohibition of processing of personal data and the anonymising, blocking, erasure or destruction of personal data whenever he concludes that the personal data are being processed in contravention of the statutory provisions; 4. to order the prohibition of the transfer of personal data to third countries, or their supply to foreign data recipients, if they are transferred or supplied in contravention of the statutory provisions or binding international treaties; 5. to order other measures provided for by the statute regulating inspection supervision and the statute regulating the general administrative procedure (Article 54 PDPA).	No information.

Spanien	Une procédure de dénonciation individuelle est prévue.	Selon le nombre qui augmente d'année en année des dénonciations, il est à supposer qu'il existe une confiance de la part du public.	Afin d'accomplir ses tâches, l'AEPD a été investie de pouvoirs d'enquête et d'inspection. Entre autre, l'AEPD peut requérir aux responsables et aux personnes chargées des traitements, après audience de ces derniers, l'adoption des mesures nécessaires à l'adéquation du traitement des données aux dispositions de la législation relative à la protection des données et, le cas échéant, ordonner la cessation des traitements et l'annulation des fichiers, en cas de non-conformité aux dispositions légales; g) exercer le pouvoir de sanction aux termes prévus dans le titre VII de la législation relative à la protection des données; h) établir les rapports, à caractère obligatoire, sur les projets de dispositions générales d'application de la législation relative à la protection des données; i) recueillir auprès des responsables des fichiers toute aide et information jugée nécessaire à l'exercice de ses fonctions; j) assurer la publicité de l'existence des fichiers des données à caractère personnel, et, à cet effet, publier périodiquement une liste desdits fichiers contenant l'information supplémentaire fixée par le directeur de l'Agence.	n/a

B. Deutschland

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) kontrolliert und berät die öffentlichen Stellen des Bundes sowie bestimmte nicht-öffentliche Stellen in Fragen des Datenschutzes und der Informationsgewährung. Die Rechtsgrundlagen seines Handelns sind vor allem das Bundesdatenschutzgesetz (BDSG) [8] und das Informationsfreiheitsgesetz. Der BfDI wird auf Vorschlag der Bundesregierung für eine Amtszeit von fünf Jahren vom Bundestag gewählt und sodann vom Bundespräsidenten ernannt. Eine einmalige Wiederwahl ist möglich.

Sein Amt versieht der BfDI nicht allein, vielmehr verfügt er über eine eigene Behörde, die organisatorisch beim Bundesministerium des Innern (BMI) angesiedelt ist. Dabei bestimmt das Gesetz, dass die Mittel des BfDI im Haushalt des BMI in einem eigenen Kapitel auszuweisen sind. So soll sichergestellt werden, dass der BfDI über die Verwendung seiner Sach- und Personalmittel ohne Einflussnahme durch das BMI entscheiden kann. Die Höhe der dem BfDI zur Verfügung gestellten Mittel muss laut Gesetz ausreichen, um ihm die Erfüllung seiner Aufgaben zu ermöglichen.

Nach der gesetzlichen Regelung im BDSG übt die Bundesregierung die Rechtsaufsicht über den BfDI aus, das Bundesministerium des Innern die Dienstaufsicht, eine Fachaufsicht besteht nicht. Nach einer starken Literaturmeinung widerspricht diese Ausgestaltung des Amtes den europarechtlichen Vorgaben zur Unabhängigkeit des Datenschutzbeauftragten, weshalb die Bestimmungen unanwendbar seien (vgl. 2.1). Dementsprechend hat die oppositionelle Fraktion Bündnis 90/Die Grünen im Deutschen Bundestag beantragt, der Bundestag möge die Regierung dazu auffordern, einen korrigierenden Gesetzesentwurf vorzulegen und die völlige Unabhängigkeit des BfDI herzustellen.[9]

Insgesamt umfasst der Mitarbeiterstab des BfDI derzeit rund 90 Personen. Mit Ausnahme des BfDI selbst, der in einem öffentlich-rechtlichen Dienstverhältnis eigener Art – mithin keinem Beamtenverhältnis, aber einem beamtenähnlichen Verhältnis – steht, handelt es sich bei den Mitarbeitern der Dienststelle um Bedienstete des BMI. Sie sind für die Dauer ihrer Arbeit beim BfDI nur diesem gegenüber weisungsgebunden, nicht den Beamten des BMI. Gleichwohl wird diese personelle Verflechtung kritisiert, da das BMI Einfluss auf die Beförderung der Mitarbeiter sowie auf deren beruflichen Werdegang nach einem möglichen Ende ihrer Beschäftigung beim Bundesbeauftragten hat.

Der BfDI wird bei der Erfüllung seiner Aufgaben unterstützt und vertreten vom Leitenden Beamten. Die Dienststelle des BfDI gliedert sich in neun Fachreferate (vgl. das Organigramm unter http://www.bfdi.bund.de/DE/Dienststelle/Organisation/organisation_node.html), die Bereiche Zentrale Aufgaben, Koordinierung/Lenkung Öffentlichkeitsarbeit und Internetredaktion sowie die Pressestelle. Die jeweiligen Zuständigkeiten der Fachreferate beziehen sich auf bestimmte Bundesbehörden oder Aufgabenbereiche einzelner Ressorts der Bundesregierung.

---

8 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I S. 2814).

9 Bundestags-Drucksache Nr. 17/6345 vom 29. Juni 2011.

Hauptaufgabe des BfDI ist es, die Daten- und Informationsverarbeitung aller öffentlichen Stellen des Bundes sowie bestimmter nicht-öffentlicher Stellen wie Telekommunikationsunternehmen, Postdienstunternehmen und Unternehmen, die unter das Sicherheitsüberprüfungsgesetz fallen, zu kontrollieren und diesen Stellen beratend zur Seite zu stehen. Ausserdem muss der BfDI den Deutschen Bundestag und die Öffentlichkeit über wesentliche datenschutzrelevante Entwicklungen im privaten Bereich unterrichten. Zu diesem Zweck verfasst er alle zwei Jahre einen Bericht für den Deutschen Bundestag. Der BfDI erteilt überdies Stellungnahmen und Ratschläge, insbesondere im Zusammenhang mit Gesetzgebungsvorhaben oder datenschutzrelevanten Verfahren vor dem Bundesverfassungsgericht.

Jedermann kann sich an den BfDI wenden, wenn er der Auffassung ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch eine vom BfDI beratenen und kontrollierten Stelle in seinen Rechten verletzt worden zu sein. Der BfDI kann selbst nur in einem Bescheid feststellen, dass der Betroffene in seinen Rechten verletzt wurde, nicht hingegen die verletzende Massnahme aufheben oder abändern. Sein Votum hat allerdings grosses Gewicht und wird im Regelfall die entsprechende Stelle zu einem rechtskonformen Verhalten bewegen (vgl. 6.1).

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	**Unabhängige Behörde, die keiner Fachaufsicht unterliegt.** Gemäss § 22 Abs. 5 BDSG untersteht der BfDI der Dienstaufsicht des Bundesministeriums des Innern (BMI). Auch wenn sich die Dienstaufsicht nur auf rein dienstliche Fragen wie Besoldung, Versorgung, Urlaub, Dienstzeit, etc. bezieht,[10] wird diese Bestimmung in der Literatur für „mit dem europarechtlichen Gebot der Unabhängigkeit der Kontrollinstanzen […] dennoch nicht vereinbar“ und daher „unanwendbar“ befunden.[11] Ähnliches gilt für die Rechtsaufsicht, also die Kontrolle der Gesetz- und Rechtmässigkeit des Verhaltens, die laut Gesetz (§ 22 Abs. 4 Satz 3 BDSG) der Bundesregierung obliegt: Auch diese Regelung hält Dammann für unanwendbar.[12]
Organisationsform	Innerhalb der Behörde 9 Fachreferate zu einzelnen Ressorts der Bundesregierung/öffentlichen Stellen, die beraten und kontrolliert werden
Grösse	Einzelperson mit Behörde, mit insgesamt rund 90 Beschäftigten.

2.2. Komplexität und Zusammenwirken der Behörden

Neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gibt es in den 16 Bundesländern **jeweils einen Landesbeauftragten für den Datenschutz**,[13] ausserdem Datenschutzbeauftragte bei den öffentlich-rechtlichen Rundfunkanstalten.[14] Die Landesbeauftragten für den Datenschutz sind dann jeweils für Fragen des Datenschutzes in den Ländern und Gemeinden zuständig, weitere zentrale öffentliche Datenschutzstellen auf regionaler oder lokaler Ebene bestehen nicht.

Zuständigkeiten für Gesetzgebung liegen jeweils bei den Parlamenten, die Datenschutzbeauftragten können keine Gesetze verabschieden. Der BfDI ist organisatorisch dem Bundesministerium des Innern (BMI) angegliedert, ohne dem BMI unterstellt zu sein. Er ist eine unabhängige Institution. Seine Mitarbeiter sind allerdings Beamte des BMI, die gegen ihren Willen während der Zeit ihrer Arbeit beim BfDI nicht auf einen anderen Posten beim BMI versetzt werden können und während ihrer Arbeit beim BfDI dessen Fachaufsicht (und nicht der des BMI) unterliegen. Die Gliederung der Behörde des BfDI selbst ist am besten aus einer Graphik ersichtlich, die über die Homepage des BfDI abrufbar ist.[15] Der BfDI ist Vorgesetzter der Mitarbeiter seiner Behörde. Er ist ihnen gegenüber weisungsbefugt.[16]

---

10 P. Gola & R. Schomerus, BDSG, 8. Aufl., München 2005, § 22 Rz. 12.

11 So U. Dallmann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 23.

12 U. Dallmann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 20.

13 Vgl. H. Garstka & D. Gill, in A. Roßnagel (Hrsg.), Handbuch Datenschutz, München 2003, 5.2 Rz. 23-38.

14 Vgl. H. Garstka & D. Gill, in A. Roßnagel (Hrsg.), Handbuch Datenschutz, München 2003, 5.3.

15 http://www.bfdi.bund.de/DE/Dienststelle/Organisation/organisation_node.html.

16 U. Dammann, in Simits (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 31.

Als nachteilhaft wird die Art der Angliederung beim BMI angesehen.[17] Ähnlich heisst es im eingangs erwähnten Antrag der Bundestagsfraktion Bündnis 90/Die Grünen: „Vor diesem Hintergrund kann nicht ausgeschlossen werden, dass die Aufsichtsfunktionen des Bundesministeriums des Innern sowie die massgebliche Rolle bei Personalentscheidungen einer unabhängigen Ausübung der Datenschutzkontrolle durch die Mitarbeiterinnen und Mitarbeiter im Einzelfall im Wege stehen kann.[18]

---

17 Vgl. dazu U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, § 22 Rz. 28: „Mit dem Gebot der Unabhängigkeit unvereinbar ist das Zusammenwirken von Bundesministerium des Innern und BfDI bei der Personalwirtschaft im Rahmen einer ‚Vebundwirtschaft'. Eine etwa 1980 getroffene interne Absprache sieht vor, dass die Personalstellen des BfDI in die Personalwirtschaft des Bundesministeriums des Innern einbezogen werden; nur bei Entscheidungen, die sein Personal berühren, ist dem BfDI eine Mitsprache eingeräumt. Damit bleibt dem BfDI zwar die dem Haushalt entsprechende Anzahl von Beamten der jeweiligen Laufbahngruppe erhalten, nicht aber die im Haushaltsplan ausgewiesenen Beförderungsämter. Der BfDI hat damit das ihm vom Gesetz eingeräumte Recht, im Rahmen der ihm zugewiesenen Haushaltsmittel eigenständig Personalentscheidungen, z. B. Stellenbesetzungen oder Beförderungen, zu treffen, eingebüsst. Die personalrechtliche Bestimmungsmöglichkeit ist aber eine für eine unabhängige Amtsführung ganz entscheidende Voraussetzung. Die Praxis ist wegen Europarechtswidrigkeit, aber auch weil sie die nach dem BDSG garantierte Unabhängigkeit unterminiert, unzulässig. Die vom seinerzeitigen Amtsträger mitgetragene Absprache ist aus formellen und materiellrechtlichen Gründen unwirksam und überdies für die nachfolgenden Amtsinhaber nicht bindend."

18 Bundestags-Drucksache Nr. 17/6345 vom 29. Juni 2011, S. 1.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	Der BfDI wird auf Vorschlag der Bundesregierung vom Bundestag gewählt und anschliessend vom Bundespräsidenten ernannt, § 22 Abs. 1 BDSG
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	Der BfDI muss zum Zeitpunkt seiner Wahl das 35. Lebensjahr vollendet haben, § 22 Abs. 1 Satz 2 BDSG. Weitere formelle Voraussetzungen bestehen nicht. Die fünfjährige Wahlperiode des BfDI entspricht nicht der (vierjährigen) Legislaturperiode des Bundestags und damit der regelmässig vierjährigen Amtsperiode einer Bundesregierung. Die Zugehörigkeit des BfDI ist weder geschriebene noch ungeschriebene Voraussetzung seiner Wahl. Zwar mag das Vorschlagsrecht der Bundesregierung dazu einladen, eine Person der eigenen Partei wählen zu lassen. Doch geschieht dies in der Praxis nicht notwendigerweise: Der derzeitige BfDI, Peter Schaar, ist Parteimitglied von Bündnis 90/Die Grünen und wurde 2003 auf Vorschlag der damals an der Regierung beteiligten Grünen in sein Amt gewählt. Die Wiederwahl erfolgte allerdings im November 2008, zu Zeiten der grossen Koalition aus CDU/CSU und SPD und mit den Stimmen der CDU/CSU. Mitgliedschaften im Verwaltungs- oder Aufsichtsrat eines auf Erwerb gerichteten Unternehmens sind nicht zulässig (vgl. hierzu sogleich unter „Zulässigkeit der Nebenbeschäftigungen“), stellen aber kein Hindernis zur Amtsübernahme dar, sondern müssen nach Amtsübernahme unverzüglich niedergelegt werden.[19]
Ausgestaltung des Arbeitsverhältnisses	Der BfDI ist dienstrechtlich kein Beamter, sondern steht in einem öffentlichrechtlichen Dienstverhältnis eigener Art (§ 22 Abs. 4 Satz 1 BDSG). Die Vorschriften des Beamtenrechts und des Bundesministergesetzes sind auf den BfDI daher nur anwendbar, soweit im Gesetz ausdrücklich auf sie verwiesen wird oder anderenfalls Lücken im Recht entstehen; im Übrigen wird das Arbeitsverhältnis durch das BDSG (bzw. bei den Landesbeauftragten für den Datenschutz durch die jeweiligen Datenschutzgesetze der Länder) ausgestaltet.[20] Die Besoldung des BfDI bemisst sich gemäss § 23 Abs. 7 BDSG nach der Besoldungsstufe B 9[21] des Bundesbesoldungsgesetzes (BBesG)
Zulässigkeit der **Nebenbeschäftigungen**	Entgeltliche Nebenbeschäftigungen sind nicht zulässig. Hierzu bestimmt § 23 Abs. 2 BDSG: „Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer

19 U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011, § 22 Rz. 9, § 23 Rz. 10.

20 U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 14.

21 Dies entspricht gemäss Anlage I zum BBesG u. a. der Besoldung des eines Ministerialdirektors als Abteilungsleiter bei einer obersten Bundesbehörde, des Präsidenten des Bundesamtes für Verfassungsschutz, des Präsidenten des Bundeskriminalamtes, des Präsidenten des Bundesnachrichtendienstes, des Präsidenten des Bundesversicherungsamtes, des Vizepräsidenten des Bundesrechnungshofes oder eine Generalleutnants der Bundeswehr.

	gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt aussergerichtliche Gutachten abgeben.“
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	keine Regelung zur Teilzeit auf Ebene des BfDI; die Frage ist bisher noch nicht praktisch aufgetaucht; möglicherweise wären die beamtenrechtlichen Bestimmungen über Teilzeit analog anzuwenden;[22] für nachgeordnete Bedienstete gelten die normalen beamtenrechtlichen Regelungen.
Länge der Amtsdauer	Die Amtsdauer des BfDI beträgt fünf Jahre mit einmaliger Wiederwahlmöglichkeit, § 22 Abs. 3 BDSG.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

Die Unzulässigkeit sämtlicher entgeltlichen Nebenbeschäftigungen wird in der Lehre kritisch kommentiert.[23] Angaben zur Möglichkeit einer Teilzeitarbeit bei der obersten Führungsstufe finden sich nicht. Offenbar ist die Frage bisher – bei den fünf BfDI, die es seit 1978 gegeben hat – nicht akut geworden.

3.3. Die Entlöhnung insbesondere

Es finden sich keine Angaben darüber, ob die Entlöhnung als adäquat empfunden wird oder nicht.

---

22 Vgl. U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 14: „Die Vorschriften des Beamtenrechts und des Bundesministergesetzes sind […] nur anwendbar, wenn ausdrücklich auf sie verwiesen wird. Soweit dabei Lücken entstehen, kommt eine Anwendung der Grundsätze des Beamtenrechts und des Dienstrechts der Bundesminister dem Rechtsgedanken nach in Betracht.“

23 U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011, § 23 Rz. 12: „Die Inkompatibilitätsregelung des Abs. 2 kann nicht als ideal bezeichnet werden. So wichtig es ist, die Objektivität des BfDI zu sichern, so wenig kann übersehen werden, dass Inkompatibilitäten zugleich den Entscheidungsspielraum bei der Kandidatenauswahl einschränken. Inkompatibilität ist insofern kein Selbstzweck und sollte nicht auf Tätigkeiten erstreckt werden, die die Objektivität typischerweise nicht tangieren. Unter diesem Gesichtspunkt wäre es angemessener, nicht auf die für den Bundespräsidenten und die Bundesminister, sondern auf die für Richter – einschliesslich der Mitglieder des Bundesverfassungsgerichts – geltende Regelung zurückzugreifen und die Tätigkeit als Hochschullehrer für vereinbar zu erklären, zumal eine ständige Verbindung mit der Wissenschaft der Tätigkeit es BfDI zugute kommen kann.“

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	Während der BfDI selbst unabhängig ist, sind seine nachgeordneten Mitarbeiter Beamten des Bundesministerium des Inneren (BMI). Für die Dauer ihrer Tätigkeit beim BfDI sind sie zwar wiederum diesem unterstellt, doch wird in der Literatur kritisch angemerkt, dass sie nach Ende ihrer Arbeit beim BfDI weiter im BMI arbeiten und befördert werden möchten.[24]
Möglichkeit der **Weisungen von aussen**	Weisungen von aussen sind gegenüber dem BfDI nicht möglich, da dieser ausserhalb der ministeriellen Hierarchie steht; gegenüber den Mitarbeitern des BfDI sind Weisungen von aussen nicht möglich, da diesen gegenüber allein der BfDI weisungsbefugt ist.
Neutralität der Behörde	Es sind keine Aussagen zu finden, die die Neutralität der Behörde in Zweifel zögen

[24] In diesem Sinne kritisch U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit. § 22 Rz. 31: „In der Praxis ist die Tätigkeit beim BfDI meist eine Durchgangsstation für Angehörige des [Innen-]Ministeriums, wo auch ihre längerfristige Berufsperspektive liegt. Es liegt auf der Hand, dass dies Auswirkungen auf die Orientierung und die Konfliktbereitschaft vieler Mitarbeiter hat. Die ‚völlige Unabhängigkeit' der Aufgabenwahrnehmung ist nicht gegeben. Die EU-Kommission hat die mit dem deutschen Modell vergleichbare organisatorische und personelle Einbindung der österreichischen Datenschutzkommission in das Bundeskanzleramt im Wege des Vertragsverletzungsverfahrens wegen Verletzung des Unabhängigkeitsgebots beanstandet. Die deutsche Regelung ist ebenso korrekturbedürftig."

5. Ressourcen

5.1. Übersicht

Budgethoheit	§ 22 Abs. 5 Satz 2 BDSG lautet: „Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen.; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen.“
Einnahmequellen der Behörde	Für Anfragen/Beschwerden von Bürgern erhebt der BfDS keine Gebühren. Anders stellt sich die Situation bei Datenschutzzertifikaten dar, die der BfDS Anbietern sogenannter „De-Mail“-Dienste ausstellt und die Voraussetzung für das Betreiben eines solchen Dienstes sind, §§ 24 Abs. 1 Nr. 2, 18 Abs. 3 Nr. 4 De-Mail-Gesetz[25].
Verfügt die Behörde **über ein eigenes Budget.**	Ja. Dass die Mittel des BdDI im Plan des BMI in einem eigenen Kapitel auszuweisen sind, hat den Zweck, dass das BMI diese Mittel nicht anderweitig verwenden kann. Über die richtige und sinnvolle Verwendung dieser Mittel entscheidet der BfDI selbst.[26]

5.2. Adäquanz des Budgets insbesondere

Es finden sich keine Informationen über die Adäquanz des Budgets für die Erfüllung der Aufgaben.

---

[25] Gesetz vom 28. April 2011, in Kraft seit dem 3. Mai 2011, BGBl I S. 666, zuletzt geändert durch Art. 2 Abs. 3 des Gesetzes vom 22. Dezember 2011, BGBl. I S. 3044.

[26] Roßnagel, Handbuch Datenschutzrecht, op. cit., 5.1 Rz. 35; U. Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 22 Rz. 26 f.

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	Nach § 21 BDSG: „Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden." Mit der Formulierung „*bei* der Erhebung etc." anstelle von „*durch* die Erhebung etc." hat der Gesetzgeber klargestellt, dass „auch die Verletzung durch Aktivitäten oder Unterlassungen geltend gemacht werden kann, die im Zusammenhang mit der Erhebung, Verarbeitung oder Nutzung steht."[27] Der BfDI ist nur für behauptete Verletzungen durch Bundesbehörden zuständig. Verletzungen durch Landesbehörden werden durch die jeweiligen Landesbeauftragten für den Datenschutz überprüft.
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	Der BfDI erteilt dem Fragesteller auf dessen Anfrage hin einen Bescheid, in dem er feststellt, ob eine Rechtsverletzung vorliegt oder nicht. Nach der Lehre handelt es sich dabei um eine Auffassung über das Vorliegen einer Datenschutzrechtsverletzung ohne unmittelbare rechtliche Wirkung, aber mit einem durch das Amt bedingten besonderen Gewicht .[28]
Weitere Aufgaben der Datenschutzbehörde	Der Bundesbeauftragte für den Datenschutz ist gleichzeitig Bundesbeauftragter für die Informationsfreiheit.

6.2. Kompetenzen der Behörde

Der BfDI übt sowohl beratende als auch kontrollierende Tätigkeit auf dem Gebiet des Datenschutzes aus. Er berät und kontrolliert alle öffentlichen Stellen des Bundes sowie als nicht-öffentliche Stellen Telekommunikations- und Postdienstleistungsunternehmen sowie private Unternehmen, die unter das Sicherheitsüberprüfungsgesetz fallen. Ausserdem ist der BfDI für die datenschutzrechtliche Beaufsichtigung der Jobcenter gemäss § 50 Abs. 2 Sozialgesetzbuch II zuständig.

Alle zwei Jahre erstellt der BfDI einen Tätigkeitsbericht, den er dem Bundestag überreicht (zuletzt der 23. Tätigkeitsbericht für die Jahre 2009 und 2010, dem Präsidenten des Bundestags am 12. April 2011 überreicht).
Zum Zusammenhang zwischen Organisationsform und Aufgaben haben sich keine spezifischen Aussagen finden lassen.

---

27 U. Dammann, in Simits (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, op. cit., § 21 Rz. 4.

28 Dammann, in Simitis (Hrsg.), Nomos-Kommentar Bundesdatenschutzgesetz, § 21 Rz. 22: „Mit dem Bescheid teilt der BfDI seine Auffassung über das Vorliegen einer (Datenschutz-)Rechtsverletzung mit. Eine unmittelbare rechtliche Wirkung auf die Rechte und Pflichten des Betroffenen oder der datenverantwortlichen Stelle geht von diesem Bescheid nicht aus. § 21 gibt dem BfDI keine Kassations-, Regelungs- oder Anordnungskompetenz. Die besondere, auf die unabhängige Stellung und auf den direkten Zugang zu Bundesregierung, Bundestag und Öffentlichkeit gestützte Autorität des Amtes verleiht den Entscheidungen gegenüber den betroffenen Behörden und Stellen jedoch ein Gewicht, das dem von Gerichtsurteilen und Weisungen vorgesetzter Behörden grundsätzlich nicht nachsteht."

6.3. Akzeptanz und Ansehen

In der Literatur finden sich keine Stimmen über das Ansehen des BfDI. Eine unsystematische Auswertung von Artikeln in den online-Archiven überregionaler Tageszeitungen ergibt, dass der BfDI als glaubwürdiger Kritiker der Regierung und grosser Konzerne (Google) auf dem Gebiet des Datenschutzes wahrgenommen wird.

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

Seit Inkrafttreten des Informationsfreiheitsgesetzes[29] am 1. Januar 2006 ist der Bundesbeauftragte für den Datenschutz auch der Bundesbeauftragte für die Informationsfreiheit. Diese Doppelrolle wird in der Literatur positiv gesehen, nämlich als „verwaltungs- und finanzökonomisch vorteilhaf[t]“.[30] Die Doppelrolle fusst auf der Erkenntnis, dass Datenschutz und Informationsgewährung zwei Aspekte der gleichen grundsätzlichen Problemlage sind.[31]

---

29 Informationsfreiheitsgesetz vom 5. September 2005, BGBl. I S. 2722.

30 H. Schmitz & S.-D. Jastrow, Das Informationsfreiheitsgesetz des Bundes, Neue Zeitschrift für Verwaltungsrecht 2005, S. 984 (985); mit gleichem Ergebnis: S. Simitis in Nomos-Kommentar zum Bundesdatenschutzgesetz, Einleitung Rz. 22, zur frühere Gesetzeslage – nach der der Bundesbeauftragte für den Datenschutz nicht gleichzeitig für die Informationsfreiheit zuständig war: „In Wirklichkeit wird […] auf diese Weise der Zusammenhang zwischen zwei eng miteinander verbundenen Fragenbereichen aufgelöst. Die Konsequenz ist eine bereits im Ansatz ebenso verzerrte wie verfehlte Sicht der Verarbeitungsprobleme.“.

31 S. Simitis in Nomos-Kommentar zum Bundesdatenschutzgesetz, Einleitung Rz. 22.

C. Frankreich

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

Créée par la **loi du 6 janvier 1978**[32] et organisée par **décret du 20 octobre 2005**[33], la **Commission nationale de l'informatique et des libertés (CNIL)** est une **autorité administrative indépendante** chargée d'assurer la protection des données et de veiller au respect de la vie privée, des libertés individuelles publiques et des droits de l'homme de manière générale.

En France, les autorités administratives indépendantes constituent des « organismes administratifs qui agissent au nom de l'Etat et disposent d'un réel pouvoir, sans pour autant relever de l'autorité du gouvernement »[34]. Elles se caractérisent par leur **pouvoir autonome de décision et d'influence** sur un secteur déterminé**,** leur **nature administrative** ce qui suppose qu'elles ont un caractère public et que les décisions qu'elles prennent aient une nature administrative. Enfin, il s'agit **d'institutions indépendantes** qui ne relèvent pas d'une autorité de contrôle et ne sont pas dépendantes d'une hiérarchie[35].

La CNIL se caractérise par son **indépendance** garantie notamment à l'article 21 de la loi du 6 janvier 1978 qui dispose que « les membres de la commission ne reçoivent d'instruction d'aucune autorité ».

La CNIL est composée de **dix-sept membres** et s'appuie sur près de **160 agents** librement recrutés par le Président de la CNIL. Parmi les dix-sept commissaires, douze sont élus par les assemblées ou les juridictions auxquelles ils appartiennent (Assemblée Nationale, Sénat, Cour de cassation, Conseil d'Etat et Conseil économique et social), cinq autres personnalités qualifiées sont désignées : trois par décret, une par le Président de l'Assemblée Nationale et une autre par le Président du Sénat. Le mandat des commissaires est de cinq ans, renouvelable une fois à l'exception des parlementaires et les conseillers économiques et sociaux siégeant pour une durée égale à leur mandat électif.

Aux termes de l'article 13 I dernier alinéa de la loi de 1978, « la commission élit en son sein un **président et deux vice-présidents**, dont un vice-président délégué. Ils composent le **bureau**. »

La CNIL dispose de **services** organisés au sein de **quatre directions**, dirigés par le président et placés sous son autorité (art.19).

S'agissant de son fonctionnement, la CNIL se réunit en **séance plénière** une fois par semaine autour de l'ordre du jour fixé par le président de la CNIL. Les membres examinent les projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement. Elle siège parfois **en formation restreinte**. Au cours de cette formation, six membres de la CNIL sont chargés d'examiner les suites à donner à certaines plaintes ou aux contrôles et adressent des mises en demeure et des avertissements.

En ce qui concerne les missions assignées à la CNIL**, l'article 11 de la loi de 1978** prévoit qu'elle est chargée de :

---

32 Loi 78-17 du 6 janvier 1978 modifiée disponible sous : http://www.cnil.fr/index.php?id=45 (13.03.2013).

33 Décret n°2005-1309 du 20 octobre 2005, disponible sous : http://www.cnil.fr/index.php?id=43 (13.03.2013).

34 Rapport public du Conseil d'Etat de 2001. Les autorités administratives indépendantes, disponible sur le site officiel de la documentation française.

35 A. Victorine Kossi, La protection des données à caractère personnel à l'ère de l'Internet, 2011, p.128-129.

- informer et conseiller les personnes sur leurs droits et obligations,
- veiller à la conformité des traitements des données à caractère personnel,
- autoriser certains traitements et recevoir des déclarations pour les autres,
- établir et publier des normes,
- recevoir des plaintes, pétitions, réclamations et informer des suites données
- répondre aux demandes d'avis des pouvoirs publics,
- rédiger et publier un rapport annuel,
- se tenir informée de l'évolution des technologies de l'information

A l'origine, la CNIL jouait un rôle d'instance de conseil et d'expertise. Peu à peu, elle s'est vue attribuer une **fonction juridictionnelle**[36]. Avec la loi du 6 août 2004 réformant la loi du 6 janvier 1978, ses pouvoirs se sont considérablement étendus notamment ceux de contrôle. Elle dispose ainsi du pouvoir :

- réglementaire et de décision.
- de donner son avis sur la conformité aux dispositions de la loi.
- de formuler des recommandations
- de faire des propositions législatives ou règlementaires
- d'apporter son concours en matière de protection des données.
- d'investigation et de contrôle.
- de saisir le juge des référés en cas d'infraction grave ou d'informer le Procureur de la République des infractions dont elle a connaissance.
- de formuler des observations lors des poursuites pour inobservation de la législation.
- de sanction administrative et pécuniaire.

Elle peut participer à la préparation et à la définition de la position française dans les négociations internationales ou à la demande du Premier ministre à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine. Elle a le pouvoir de délivrer un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

Au fils du temps, les missions de la CNIL se sont amplifiées[37] mais sa structure n'a pas beaucoup évolué.

---

36 Voir CE, Ord. réf., 19 févr. 2008, req. n°311974, Société Profil France, Le Conseil d'Etat a ainsi qualifié la CNIL « de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales en raison de sa nature et de son organisation.

37 Voir Rapport d'activité 2011 de la CNIL, éd. 2012, p. 7. Depuis 2011, la CNIL s'est vu attribuer deux nouvelles compétences. La première a été introduite par l'article 18 de la loi du 14 mars 2011 dite LOPPSI 2, qui attribue à la CNIL la compétence pour contrôler tous les systèmes de vidéo protection installés sur la voie publique en application de la loi du 21 janvier 1995.La seconde procède à la transposition de la directive révisant le « paquet télécom » qui a introduit l'obligation de notifier les violations des données à caractère personnel à la CNIL (article 38 de l'ordonnance n°2011-1012 du 24 août 2011).

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	La CNIL est une **autorité administrative indépendante** créée par la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 et organisée par le décret du 20 octobre 2005. Elle se caractérise par son **indépendance**. A cet égard, **l'article 21, alinéa 1** de la loi de 1978 dispose que «dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité». Elle jouit d'une marge de manœuvre importante, le seul contrôle dont elle relève est celui du juge. En principe, le gouvernement n'exerce ni tutelle, ni pouvoir hiérarchique. La CNIL reste toutefois une institution de l'Etat, dénuée de personnalité morale et le législateur peut modifier ses pouvoirs dans le respect du principe de liberté individuelle[38].
Organisationsform	S'agissant de sa forme, la CNIL constitue un **organisme collégial de portée nationale** comprenant notamment un président, un vice-président et un vice-président délégué. Son siège se trouve à Paris. La CNIL dispose de **services dirigés par le président** et placés sous son autorité (art.19). Ils sont organisés au sein de **quatre directions** : - Direction des études, de l'innovation et de la prospective - Direction des affaires juridiques, internationales et de l'expertise - Direction des relations avec les usagers et du contrôle - Direction des ressources humaines, financières, informatiques et logistiques
Grösse	Elle est composée **de dix-sept membres** : parlementaires, hauts fonctionnaires, magistrats, personnalités qualifiées (art. 13 I de la loi). Elle s'appuie sur près **de 160 agents** librement recrutés par le Président de la CNIL[39].

2.2. Komplexität und Zusammenwirken der Behörden

En France, le contrôle exercé en matière de protection des données est un **contrôle centralisé** contrairement à l'Allemagne où le contrôle est effectué de manière décentralisée. Afin d'éviter aux entreprises la contrainte d'une déclaration CNIL dès lors qu'un traitement de données personnelles est mis en place, la désignation **d'un correspondant CNIL** au sein des entreprises a été prévue par le législateur français.

Plus précisément, en transposant la directive communautaire 95/46/CE du 24 octobre 1995, l'article 22 II de la loi du 6 août 2004, qui modifie la loi du 6 janvier 1978 « Informatique et libertés», a

38 A. Victorine Kossi, op. cit., p.128-129.

39 Chiffre issu du site officiel de la CNIL disponible sous : http://www.cnil.fr/ (08.03.2013).

instauré la possibilité pour les entreprises de nommer un **Correspondant Informatique et Libertés (CIL)** aussi appelé « Correspondant à la protection des données personnelles (CPDP) »[40].

Les responsables de fichiers peuvent désigner un CIL. Il s'agit d'une personne qui « bénéficie des qualifications requises pour exercer ses missions »[41].

Le CIL permet de **garantir la conformité de l'organisme à la loi Informatique et Libertés**. Il a pour mission d'assurer que toutes **les précautions utiles ont été prises pour préserver la sécurité des données** et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des personnes non autorisées y aient accès. Des outils sont mis à disposition du CIL pour l'aider dans cette tâche[42].

La CNIL conduit une vaste opération de communication et de pédagogie auprès des acteurs concernés par la désignation d'un CIL. Les plus grandes entreprises françaises sont invitées à se doter de correspondants, ainsi que les collectivités locales.

S'agissant des attributions législatives, la **CNIL est consultée sur tout projet de loi** ou de décret relatif à la protection des personnes à l'égard des traitements automatisés.

Plus largement, elle donne également **un avis sur la conformité à la loi des projets** de règles professionnelles et produits et procédures protectrices des données personnelles ou tendant à leur anonymisation. Deux avis ont été donnés par la CNIL sur des règles professionnelles.

Elle peut **proposer** au Gouvernement des **mesures législatives ou réglementaires** d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques (l'article 11 4° b).
À la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données.

Enfin, ses compétences et son autorité reconnue lui valent de pouvoir être associée, à la demande du Premier ministre, à la **préparation et à la définition de la position française** dans les négociations internationales intéressant le domaine de la protection des données personnelles. De la même façon, elle peut **participer à la représentation française** dans les organisations internationales compétentes en ce domaine.

Certains pouvoirs sont réservés au **président de la CNIL**. Ainsi, le président de la commission peut **mettre en demeure une personne** en vue de faire cesser le manquement constaté dans un délai qu'il fixe. Il peut demander au bureau de rendre publique la mise en demeure (art.45).

Par ailleurs, la Commission peut charger le président ou le vice-président délégué d'exercer certaines attributions (art. 15 alinéa 3) telles que **la vérification des garanties** présentées par le demandeur (art. 64).

---

40 Voir Article A. Benoussan, Gazette du Palais, 19 avril 2005 n° 109, p. 10.

41 Voir Les guides de la CNIL - Guide du correspondant informatique et libertés, éd. 2011, p. 6, disponible sous : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_correspondants.pdf (12.03.2013) ; Compte rendu de la Réunion d'information du CIL - Octobre 2012 disponible sous : http://www.cil.cnrs.fr/CIL/IMG/pdf/presentation_cil_dr_oct_2012.pdf (12.03.2013).

42 Voir Les guides de la CNIL, op. cit., p. 3, disponible sous : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_correspondants.pdf (12.03.2013).

En formation plénière, **la voix** du président est **prépondérante** (art. 15 alinéa 2). Il **dirige les services** de la Commission et nomme les agents. Il a sous son autorité le secrétariat général (art. 19). Il prend certaines décisions telles que le report de délai.

Il peut **décider de l'assistance d'un expert** dans l'accomplissement des missions de la commission (art. 44).

Aux termes de l'article 45 de la loi du 6 janvier 1978, « en cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés ». Il peut être appelé par la juridiction d'instruction ou de jugement à déposer ses observations ou à les développer oralement à l'audience.

A la suite de la demande du législateur européen qui a sollicité la mise en place d'une autorité assurant la protection des données[43], le législateur français a établi une autorité administrative indépendante par le truchement de la loi du 6 janvier 1978 dite « loi informatique et libertés ». Cette loi a institué la CNIL qui assume le respect et le contrôle de la protection des données. Au fils des années, il y a eu à la fois une **amplification de ses missions** par des interventions législatives successives mais aussi **une sauvegarde de sa structure** malgré les réformes. Elle a notamment subi d'importantes mutations avec la réforme du 6 août 2004 dotant le CNIL de très larges pouvoirs de sanction administrative et pécuniaire.

L'indépendance des membres de la CNIL est garantie de manière explicite par deux dispositions de la loi du 6 janvier 1978.

Ainsi, **l'article 21, alinéa 1** dispose que « dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité ».

L'indépendance de la CNIL est renforcée à **l'article 14** qui prévoit que :« 1) la qualité de membre de la CNIL est incompatible avec celle de membre du gouvernement ;
2) qu'aucun commissaire ne peut participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il détient ou a détenu au cours des trente-six mois antérieurs, un intérêt direct ou indirect, exercé des fonctions ou détenu un mandat. (…) ».

La Commission précise, sur son site officiel, que l'indépendance de la CNIL est garantie par sa composition et son organisation[44].

Il n'existe pas de disposition spécifiant la neutralité de l'autorité. Toutefois, le Conseil d'Etat, dans son **ordonnance de référé rendue 19 février 2008**[45], a considéré que la Commission, « eu égard à sa nature, à sa composition et à ses attributions » doit « être qualifiée de **tribunal** au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ». La CNIL est donc une autorité impartiale, elle ne représente pas un groupe d'intérêts particulier.

Les **inconvénients** résultent de **l'amplification de l'activité de la CNIL** notamment depuis la réforme de 2004 alors que **celle-ci manque de moyens** (financiers et humains).
A titre d'exemple, depuis 2004, les procédures de sanctions peuvent être engagées devant la formation spécialisée de la CNIL. Ces procédures sont assorties de rigoureuses garanties formelles.

---

43 Art. 21 alinéa 1 de la directive 95/46/CE.

44 Disponible sous : http://www.cnil.fr/la-cnil/qui-sommes-nous/ (12.03.2013).

45 CE, Ord. réf., 19 févr. 2008, req. n°311974, Société Profil France op. cit.

En conséquence, la gestion administrative de la CNIL est alourdie. On peut constater un poids des charges procédurales et de gestion. Ceci entraine un alourdissement des besoins de la CNIL en personnel et en budget. Il y a donc une structuration voire rigidification de ses méthodes alors que ces missions essentielles impliquent adaptation constate de ses capacités d'analyse à des sujets évolutifs.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	La CNIL est composée de **dix-sept membres** (art. 13 I), dont les modes de nomination varient. Elle comprend ainsi deux députés et deux sénateurs, désignés respectivement par leurs assemblées ; deux membres du Conseil économique, social et environnemental, élus par cette assemblée ; deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ; deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ; deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ; trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ; deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat . La CNIL est placée sous l'autorité d'un président, élu par les membres de la commission . Le président, ainsi que deux vice-présidents et un vice-président délégué composent le bureau de la Commission . Le président attribue à chaque commissaire un secteur en fonction de ses compétences .
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	Le président de la CNIL recrute librement ses collaborateurs. Bien souvent, il s'agit de personne **qualifiée en droit** (juriste) et **en informatique**[46]. Les membres sont **indépendants**. Ceci est caractérisé par l'inamovibilité et l'incompatibilité qui les frappent. En effet, en application de l'art 14 I de la loi, « la qualité de membre de la commission est incompatible avec celle de membre du Gouvernement ». Le II de cet article précise qu' « aucun membre de la commission ne peut : participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il détient un intérêt, direct ou indirect, exerce des fonctions ou détient un mandat ; participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il a, au cours des trente-six mois précédant la délibération ou les vérifications, détenu un intérêt direct ou indirect, exercé des fonctions ou détenu un mandat.

[46] Art. 13 de la loi du 6 janvier 1978 modifiée.

	III. Tout membre de la commission doit informer le président des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale. Ces informations, ainsi que celles concernant le président, sont tenues à la disposition des membres de la commission. Le président de la commission prend les mesures appropriées pour assurer le respect des obligations résultant du présent article ».
Ausgestaltung des Arbeitsverhältnisses	Il s'agit de parlementaires, de fonctionnaires, de magistrats et des personnalités qualifiées dans certains types de domaine tel que l'informatique. (cf. 3.1 Ernennung der Behördenmitglieder)
Zulässigkeit der **Nebenbeschäftigungen**	L'article 28 du Règlement Intérieur de la CNIL prévoit que « dans le mois qui suit son entrée en fonctions, chaque membre de la commission informe le président des intérêts directs ou indirects qu'il détient, des fonctions qu'il exerce et de tout mandat qu'il détient au sein d'une personne morale. En cours de mandat, il informe le président des intérêts directs ou indirects qu'il vient à détenir, des fonctions qu'il vient à exercer et de tout mandat qu'il vient à détenir au sein d'une personne morale dans le mois qui suit la modification de sa situation. Le président est tenu, dans les mêmes délais, de déclarer par écrit les informations le concernant. Elles sont communiquées aux autres membres du bureau. Les informations relatives aux membres ainsi que celles concernant le président sont conservées par le secrétaire général dans des conditions qui en garantissent la confidentialité. Elles peuvent être consultées sur place par les membres de la commission et par le commissaire du Gouvernement. »
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	La loi ne prévoit pas de règles spécifiques concernant le type de contrat de travail (plein temps, temps partiel).
Länge der Amtsdauer	Selon l'article 13 II de la loi, le mandat des membres de la commission est de cinq ans ; il est renouvelable une fois à l'exception des membres issus du Conseil économique et social, de l'Assemblée Nationale et du Sénat qui sont élus pour une durée égale à celle de leur mandat dans leurs institutions respectives[47].

[47] A. Victorine Kossi, op. cit. p. 129.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

Il n'y a pas d'indications doctrinales à ce sujet.

3.3. Die Entlöhnung insbesondere

En ce qui concerne la rémunération des membres de la CNIL, il a été rapporté par la presse[48], que la Cour des comptes, dans son rapport d'observations provisoires datant de fin 2010, non communicable au public, aurait contesté la rémunération du Président de la CNIL et de ses commissaires, comme les indemnités de déplacement des contrôleurs et aurait sollicité le remboursement des sommes en trop perçues.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	Selon l'article 11 alinéa 1, la CNIL est une « autorité administrative indépendante ». Elle est en France la première institution de ce type à avoir été créée. Son budget est rattaché aux services du premier ministre, ainsi elle dispose des crédits nécessaires à son activité mais elle reste autonome dans leur gestion. En outre, sur le plan du fonctionnement de l'institution, la présence d'un commissaire du gouvernement trahit l'appartenance de la CNIL à l'administration française. Les agents de la CNIL sont des agents contractuels de l'Etat. Le droit administratif s'applique à une institution telle que la CNIL : ses décisions sont susceptibles de faire l'objet d'un recours devant le juge administratif ; les dommages qu'elle pourrait causer engagent la responsabilité de l'Etat.
Möglichkeit der **Weisungen von aussen**	La CNIL ne reçoit d'instruction d'aucune autorité, ni de l'Etat . Mais elle est consultée par les autorités publiques, y compris par les juridictions. Elle doit répondre à toute demande d'avis de leur part . Elle est également susceptible d'apporter son concours aux autres autorités administratives indépendantes . La CNIL est consultée par le gouvernement sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés . Elle peut aussi proposer au gouvernement des mesures réglementaires ou législatives. Enfin, sur demande du premier ministre, elle peut contribuer à la définition de la position française dans les négociations internationales . La CNIL doit présenter annuellement un rapport au Président de la République, au Premier ministre et au Parlement rendant compte de l'exécution de sa mission . La CNIL n'est tenue d'aucune autre obligation envers une quelconque autorité, sauf, comme tout organisme public, la reddition des comptes devant la Cour des comptes. Aucune autorité n'est en droit de délivrer une instruction à la CNIL ou à ses commissaires dans l'exercice de leurs attributions.
Neutralität der	Un certain nombre d'incompatibilités assure l'indépendance des

[48] Voir article F. Johannes, La CNIL dans le collimateur de la Cour des comptes, lemonde.fr du 25.01.2011 disponible sous http://www.lemonde.fr/societe/article/2011/01/25/la-cnil-dans-le-collimateur-de-la-cour-des-comptes_1470172_3224.html (11.03.2013).

Behörde	commissaires de la CNIL. La qualité de membre de la commission est incompatible avec celle de membre du gouvernement. En outre, un membre de la commission ne peut plus exercer ses fonctions dès lors qu'il a détenu un intérêt, direct ou indirect, a exercé des fonctions ou a détenu un mandat dans l'organisme objet du contrôle dans les trente-six mois précédant la délibération ou les vérifications de la CNIL. Enfin, tout membre de la commission doit informer le président des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale .

5. Ressourcen

5.1. Übersicht

Budgethoheit	La CNIL dispose d'une autonomie budgétaire (art 12 de la loi du 6 janvier 1978 « elle dispose des crédits nécessaires à l'accomplissement de ses missions ») mais n'a pas d'indépendance financière puisque le budget de la CNIL dépend du ministère de la Justice[49]. Il s'élève à 16 millions d'€ de budget[50].
Einnahmequellen der Behörde	Il n'y a pas de frais. La déclaration des fichiers à la CNIL est gratuite.
Verfügt die Behörde **über ein eigenes Budget.**	L'article 12 de la loi du 6 janvier 1978 énonce seulement que « la Commission nationale de l'informatique et des libertés dispose des crédits nécessaires à l'accomplissement de ses missions ». Les comptes de la commission sont présentés au contrôle de la Cour des comptes, même si la loi du 10 août 1922 relative au contrôle financier n'est pas applicable à leur gestion .

5.2. Adäquanz des Budgets insbesondere

Certains auteurs ont dénoncé le **manque de moyens alloués à la CNIL** quand bien même des efforts constants ont été réalisés par la Commission afin d'assurer ses missions[51]. La Cour des comptes a cependant relevé dans son rapport d'observations provisoires (établi fin 2010) une mauvaise gestion financière et a pointé du doigt la rémunération des membres de l'autorité[52].

49 Article D. Forest, Proposition de règlement communautaire : l'indépendance de la CNIL questionnée, Revue Lamy Droit de l'Immatériel, Juillet 2012, n°84, n° 2840.

50 Chiffre issu du site officiel de la CNIL disponible sous : http://www.cnil.fr/la-cnil/qui-sommes-nous/ (12.03.2013).

51 J. Huet, op. cit., p.13-21.

52 Article F. Johannes, La CNIL dans le collimateur de la Cour des comptes, op. cit.

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen ¨ (andere Behörden, Unternehmen, Privatpersonen)	Tout citoyen peut s'adresser à la CNIL pour : - adresser une **plainte** en cas de violation de la loi informatique et libertés - **accéder aux informations** contenues dans des fichiers de police ou de gendarmerie. - **demander les coordonnées** d'un responsable de fichier auprès de qui exercer ses droits[53]. L'article 11 2° c) dispose que la CNIL « reçoit les **réclamations, pétitions et plaintes** relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ».
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	La CNIL a la **faculté de saisir le juge des référés** en cas d'atteinte grave (art 45). Elle peut informer le procureur de la République des infractions dont elle a connaissance et émettre des observations au cours de la procédure pénale (art. 11 2° e). La CNIL dispose d'un **pouvoir de recommandation**. Elle « peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi » (art. 11). Elle peut émettre des décisions individuelles ou règlementaires dans certaines conditions (art. 45). Elle dispose d'un **pouvoir de propositions législatives et réglementaires** (art. 11 4° b). Elle a **un pouvoir d'investigation et de vérification** et peut procéder à des contrôles sur place (art. 11 2° f). La CNIL a un **pouvoir de sanction administrative et financière**. En effet, elle est compétente pour délivrer un avertissement, mettre en demeure, prononcer des sanctions pécuniaires, enjoindre de cesser un traitement ou retirer une autorisation (art. 45). Depuis 2011, elle est compétente pour contrôler tous les systèmes de vidéo protection installés sur la voie publique.
Weitere Aufgaben der Datenschutzbehörde	En application de l'article 11 de la loi du 6 janvier 1978, elle est chargée : - d'informer toute personne et tout responsable de traitement de ses droits et obligations, -de garantir le droit d'accès aux fichiers et de recenser les fichiers, -de veiller à la conformité des traitements de données à caractère personnel aux exigences légales.

[53] Consulter le site de la CNIL sur les droits des citoyens, disponible sous : http://www.cnil.fr/vos-libertes/vos-droits/ (12.03.2013).

	- d'autoriser certains traitements et de recevoir des déclarations pour les autres - d'établir et de publier des normes (art. 11 2° b) - de conseiller les pouvoirs publics, autres autorités administratives indépendante et juridictions ainsi que toute personnes et organise intéressés. - délivrer des labels à des produits ou procédures renforçant la qualité des traitements de données à caractère personnel. - de se tenir informée de l'évolution des technologies de l'information et publier ses appréciations sur les conséquences (art. 11 4°).

6.2. Kompetenzen der Behörde

La CNIL est investie, au vu de l'article 11 de la loi de 1978, d'une **mission d'information du public** sur ses droits ainsi que d'une **mission de conseil**. A cet égard, elle répond aux demandes d'avis des pouvoirs publics et des juridictions.

La CNIL veille à ce que les traitements de données à caractère personnel soient conformes à la loi ce qui suppose l'exercice d'un **contrôle a posteriori** de la CNIL. Elle donne son autorisation dans les cas prévus par la loi et qui présentent des risques pour les libertés. Par ailleurs, elle effectue certains contrôles a posteriori. Enfin, elle dispose d'un pouvoir de sanction administrative et pécuniaire ainsi que d'un pouvoir d'injonction (article 45 I 2°) qui s'est amplifié avec la réforme de 2004.

Il n'existe pas de texte permettant d'établir les ressources utilisées pour chaque tâche. Certaines tâches sont réservées au Président de la CNIL (cf. 2.3)

6.3. Akzeptanz und Ansehen

De manière générale, la CNIL a longtemps jouit d'une bonne réputation. En effet, la loi instaurant cette autorité indépendante est considérée comme pionnière et a entrainé l'adoption de textes comparables dans d'autres Etats européens[54]. Elle apparait comme une autorité « exemplaire puisque son modèle s'est généralisé en Europe et dans d'autres pays »[55]. Les auteurs estiment que la CNIL remplit «globalement bien » ses missions telles que définies par la loi et ce malgré l'insuffisance des moyens mis à sa disposition[56].

Tenant compte de l'évolution permanente des nouvelles technologies et partant de ses propres missions, elle se remet souvent en question. En ce qui concerne sa mission d'alerte et d'information, la CNIL s'efforce de diffuser ses recommandations ainsi que les sujets qui la préoccupe. Ainsi, elle attire l'attention toute particulière des médias « grâce à son indépendance, à la pertinence de ses analyses et propositions, à l'actualité de ses diagnostics sur les évolutions en cours, à l'équilibre de ses appréciations »[57].

Un sondage effectué en 2007 révèle pourtant que la CNIL ne jouit pas d'une grande notoriété auprès du public qui parfois ignore son existence ou se sent insuffisamment informé de ses droits[58].

---

54 A. Gruber, Le système français de protection des données personnelles, op. cit., p. 4.

55 J. Huet, op. cit., p.14

56 . Huet, op. cit., p.14

57 J . Huet, op. cit., p. 16-17.

58 Voir sondage accomplie en 2007, J. Huet, op. cit., p. 14.

Par ailleurs, n'étant plus soumis à l'exigence d'avis conformes de la CNIL, il apparait que les autorités publiques depuis quelques années s'écartent de plus en plus des recommandations de celle-ci[59].
Enfin, récemment, l'ex président du Conseil national du numérique aurait critiqué la CNIL pour sa régularisation excessive et il aurait sollicité sa fermeture[60].

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

La France privilégie la protection des données personnelles en recherchant un juste équilibre entre la libre circulation des informations et le respect de la vie privée[61]. La CNIL a donc été chargée d'assurer la protection des données personnelles et de veiller à ce que le développement des nouvelles technologies ne porte pas atteinte aux libertés individuelles et publiques. En ce qui concerne cette double mission, une critique a été émise par le Président de la CNIL en 1998, s'agissant de la directive européenne de 1995 qui qualifie la CNIL et ses homologues d' « autorité de contrôle ». Il regrette que ce texte insiste davantage sur la mission de protection des personnes qui s'est développée au fils du temps (notamment du fait de l'accroissement de ses pouvoirs de contrôle et de sanction) alors que la Commission devrait, selon lui, conserver son rôle d'« Académie des Libertés »[62].

---

59 Par exemple, contre l'avis de la CNIL, il a été décidé de la création du fichier Edvige qui permet la conservation de données sur des adolescents susceptibles de troubler l'ordre public.

60 Voir site officiel de l'Institut Montaigne. Gille Babinet a récemment lancé une attaque contre la CNIL lors d'un entretien mis en ligne sur le site de l'Usine Nouvelle en sollicitant sa fermeture, disponible sous : http://www.institutmontaigne.org/l-usine-nouvelle-26-fevrier-2013-3722.html (11.03.2013).

61 A. Victorine Kossi, op. cit., p.129 ; A. Gruber, op. cit., p. 4.

62 Voir G. Braibant, Données personnelles et société de l'information, Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998, disponible sous : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/984000836/0000.pdf (12.03.2013).

D. Italien

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

Il Garante per la protezione dei dati personali è un'**autorità amministrativa indipendente**[63] – istituita con legge 31 dicembre 1996, n. 675 (c.d. legge sulla privacy)[64] – disciplinata dal **D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali** (c.d. codice della privacy).

Le autorità amministrative indipendenti (la cui denominazione come categoria non ha esplicite basi normative ma è di ricostruzione dottrinale) sono organismi che esercitano le loro funzioni in ambiti considerati sensibili e di alto contenuto tecnico (concorrenza, privacy, comunicazioni ecc.), tali da esigere una peculiare posizione di autonomia e di indipendenza nei confronti del Governo, allo scopo di garantire una maggiore imparzialità (cd. neutralità) rispetto agli interessi coinvolti.

Il Garante per la protezione dei dati personali, in particolare, è una autorità di garanzia, cioè posta a tutela dell'esercizio di diritti fondamentali (mentre altre autorità amministrative indipendenti sono autorità di regolazione e vigilanza, volte ad assicurare il contraddittorio paritario degli operatori economici in un determinato mercato a tutela degli utenti e dei consumatori).

Il **Garante** per la protezione dei dati personali è un **organo collegiale**, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile[65]. L'attuale Collegio si è insediato il 19 giugno 2012.

Alle dipendenze del Garante è posto l'**Ufficio del Garante**[66], articolato in **dipartimenti**[67] e **servizi**[68]**,** oltre che in alcune **unità temporanee**[69]. Sovrintende all'Ufficio il **Segretario generale**.

---

63 Nonostante non siano riconducibili ad un archetipo, o ad un modello di carattere generale, le autorità presentano alcuni tratti comuni, come l'autonomia organizzativa e regolamentare, e la potestà normativa, sanzionatoria e di risoluzione e aggiudicazione di conflitti. Inoltre, esse sono caratterizzate da un regime particolare di incompatibilità e da peculiari regole di garanzia, volte a evitare interferenze di natura politica. V. http://www.treccani.it/enciclopedia/autorita-amministrative-indipendenti/; POTO, voce Autorità amministrative indipendenti, in Dig. disc. pub., 2008, disponibile sulla banca dati http://pluris-cedam.utetgiuridica.it; CARINGELLA, Corso di diritto amministrativo, Tomo I, Milano, 2011, 1085 ss.

64 Tale legge ha attuato la direttiva comunitaria 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

65 Art. 153 D.Lgs. 196/2003.

66 Art. 156 D.Lgs. 196/2003. Il secondo comma della disposizione citata prevede che "Il ruolo dell'organico del personale dipendente è stabilito nel limite di cento unità".

Si tratta dei seguenti dipartimenti: dipartimento realtà economiche e produttive; dipartimento comunicazioni e reti telematiche; dipartimento risorse umane; dipartimento amministrazione e contabilità; dipartimento contratti e risorse finanziarie; dipartimento attività ispettive e sanzioni; dipartimento risorse tecnologiche; dipartimento registro dei trattamenti. Per una sintetica descrizione dei singoli ambiti di attività v. http://www.garanteprivacy.it/web/guest/home/autorita/ufficio

I servizi sono i seguenti: servizio segreteria del collegio; servizio relazioni istituzionali; servizio relazioni comunitarie e internazionali; servizio relazioni con i mezzi di informazione; servizio studi e documentazione; ufficio relazioni con il pubblico (Urp). Per una sintetica descrizione dei singoli ambiti di attività v. http://www.garanteprivacy.it/web/guest/home/autorita/ufficio

69 Si tratta della: unità ricorsi; unità organizzazione e controllo di gestione; unità affari legali e di giustizia; unità informazione e documentazione comunitaria e internazionale; unità lavoro pubblico e privato; progetto formazione. Per una sintetica descrizione dei singoli ambiti di attività v. http://www.garanteprivacy.it/web/guest/home/autorita/ufficio

Il Garante si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali. Tra i suoi compiti rientrano, tra l'altro, quelli di[70]:

- controllare che i trattamenti di dati personali siano conformi a leggi e regolamenti e, eventualmente, prescrivere ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento;
- esaminare reclami e segnalazioni nonché decidere i ricorsi presentati ai sensi dell'articolo 145 del Codice in materia di protezione dei dati personali;
- vietare in tutto od in parte, ovvero disporre il blocco del trattamento di dati personali che per la loro natura, per le modalità o per gli effetti del loro trattamento possano rappresentare un rilevante pregiudizio per l'interessato;
- adottare i provvedimenti previsti dalla normativa in materia di dati personali, tra cui, in particolare, le autorizzazioni generali per il trattamento dei dati sensibili;
- promuovere la sottoscrizione dei codici di deontologia e di buona condotta in vari ambiti (credito al consumo, attività giornalistica, ecc.);
- segnalare, quando ritenuto opportuno, al Governo la necessità di adottare provvedimenti normativi specifici in ambito economico e sociale;
- partecipare alla discussione su iniziative normative con audizioni presso il Parlamento;
- formulare i pareri richiesti dal Presidente del Consiglio o da ciascun ministro in ordine a regolamenti ed atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice;
- predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla *privacy* da trasmettere al Parlamento e al Governo;
- partecipare alle attività comunitarie ed internazionali di settore, anche quale componente del Gruppo Articolo 29 e delle Autorità comuni di controllo previste da convenzioni internazionali (Europol, Schengen, Sistema informativo doganale);
- curare la tenuta del registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37 del Codice in materia di protezione dei dati personali;
- curare l'informazione e la sensibilizzazione dei cittadini in materia di trattamento dei dati personali, nonché sulle misure di sicurezza dei dati;
- coinvolgere i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.

[70] V. il sito http://www.garanteprivacy.it/web/guest/home/autorita/compiti

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Autorità amministrativa indipendente istituita con l. 675/1996 e attualmente disciplinata dal D.Lgs. 196/2003.
Organisationsform	Il **Garante** per la protezione dei dati personali è un **organo collegiale**. Alle dipendenze del Garante è posto l'**Ufficio del Garante**, struttura amministrativa articolata in dipartimenti, servizi e unità temporanee, cui è preposto un **Segretario generale**. La forma di organizzazione dell'Autorità garante per la protezione dei dati personali è disciplinata, oltre che dagli articoli 153 ss. D.Lgs. 196/2003, dal Regolamento del Garante n. 1/2000[71].
Grösse	Il Garante è organo collegiale costituito da **quattro** membri: un presidente, un vice presidente e due componenti (art. 153 D.Lgs. 196/2003). Il ruolo organico del personale dipendente dell'Ufficio del Garante è stabilito nel limite di **cento** unità[72]. L'Ufficio può avvalersi, per motivate esigenze e alle condizioni previste dalla legge, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o simile, in numero non superiore, complessivamente, a **venti** unità, lasciando non coperto un corrispondente numero di posti di ruolo. In aggiunta al personale di ruolo l'Ufficio può assumere dipendenti con contratto a tempo determinato, in numero non superiore a venti unità (art. 156 D.Lgs. 196/2003).

2.2. Komplexität und Zusammenwirken der Behörden

Il Garante per la protezione dei dati personali è un'autorità di rilievo nazionale. L'Autorità garante per la protezione dei dati personali opera in piena autonomia e con indipendenza di giudizio e di valutazione. Tra i suoi compiti rientra quello di segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti fondamentali anche a seguito dell'evoluzione del settore[73]. La legge prevede che il Presidente del Consiglio dei ministri e ciascun ministro consultino il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal "Codice della privacy"[74].

Il Garante è organo collegiale composto da quatto membri. Il Presidente: a) rappresenta il Garante; b) convoca le riunioni del Garante, ne stabilisce l'ordine del giorno, designa i relatori e dirige i lavori; c) promuove le liti e vi resiste relativamente agli atti di competenza propria o del collegio, ed ha il potere di conciliare e transigere; d) coordina l'attività die componenti nei rapporti con il Parlamento e con gli altri organi costituzionali o di rilievo costituzionale, nell'attività di comunicazione pubblica,

---

71 Consultabile al sito : http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1098801

72 L'art. 1, comma 2, L. 27 dicembre 2006, n. 296, autorizza il Garante ad incrementare la propria dotazione organica in misura non superiore al 25 per cento della consistenza prevista dall'art. 156, comma 2 , del D.Lgs. 196/2003. Nel 2008 l'Autorità ha dato concreta attuazione alla deliberazione di incremento della pianta organica che ha potenziato di **venticinque unità** la dotazione organica dell'Ufficio.
http://www.wps-group.it/privacy/288-provvedimenti_privacy-Deliberazione-n-34-Incremento-pianta-organica-dellAuto.php

73 Art. 154, comma 1, lett. f, D.L.gs. 196/2003.

74 Art. 154, comma 4, D.Lgs. 196/2003.

nonché nelle relazioni con le autorità indipendenti e di vigilanza, con le pubbliche amministrazioni, con le autorità di controllo degli altri Paesi, con gli organi dell'Unione europea e del Consiglio d'Europa e con gli altri organismi internazionali (art. 3, comma 2, *Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali*). Il voto del presidente prevale in caso di parità (art. 153, comma 3, D.Lgs. 196/2003).

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla L. 31 dicembre 1996, n. 675, che ha attuato la direttiva comunitaria 95/46/CE.

La scelta di tale forma organizzativa risponde alla necessità di approntare strutture operative caratterizzate dalla garanzia di imparzialità e da una conoscenza tecnico-giuridica più specifica, in settori della vita economico-sociale che richiedono l'esercizio di poteri di garanzia, di vigilanza e di bilanciamento di interessi che rivestono un preminente interesse per la collettività[75].

Tra le modificazioni che hanno riguardato questo organismo si segnalano le seguenti: l'originaria denominazione "Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" è stata semplificata con il D.Lgs. 9 maggio 1997, n. 123; la durata in carica del presidente e dei componenti del Garante era di quattro anni, con possibilità di rinnovo dell'incarico per una sola volta[76]. Inoltre, nel tempo si sono intensificati i poteri sanzionatori, in particolare quelli diretti a comminare sanzioni pecuniarie, volti a garantire l'effettivo rispetto delle norme da parte degli operatori[77].

L'autonomia e l'indipendenza di giudizio e di valutazione che, per espressa previsione legislativa, caratterizzano il Garante (art. 153, comma 1, D.Lgs. 196/2003), sono assicurate dalla procedura prevista per la nomina dei membri; dai requisiti soggettivi dei candidati; dalle condizioni stabilite per il loro mandato; dalla previsione di un trattamento economico commisurato, in diversa proporzione, alle supreme magistrature (art. 153, comma 4)[78].

Non si rinvengono informazioni ufficiali circa le opinioni dei principali gruppi di interesse in ordine alla neutralità dell'Autorità garante della privacy rispetto ad influenze provenienti dalla politica.

Esiste uno studio condotto dalla Camera dei deputati, avente ad oggetto, in generale, "le autorità amministrative indipendenti", che recepisce le opinioni di un'ampia platea di soggetti[79]. Emerge dall'indagine che i maggiori rischi di condizionamento da parte della politica si annidano sul piano delle nomine. È opinione condivisa che costituisca un buon presidio dell'indipendenza la previsione di processi di nomina degli organi di vertice delle autorità che non affidino la scelta al solo apparato

---

75 Cfr. la Relazione annuale 1997, par. 3.2., http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1343350.

76 L'art. 47-quater del decreto legge del 31 dicembre 2007, n. 248, convertito, con modificazioni, dalla legge 27 febbraio 2008, n. 31, ha stabilito che la durata in carica del presidente e dei componenti del Garante è di sette anni e che gli incarichi non sono rinnovabili (la disposizione è stata introdotta per equiparare la durata in carica del presidente e dei componenti del Garante a quella prevista per altre autorità indipendenti, con decorrenza dalla data del decreto di nomina, eliminando la possibilità di essere confermati nell'incarico).

77 Cfr. l'Indagine conoscitiva sulle autorità amministrative indipendenti, condotta dalla Camera dei deputati, Doc. XVI, n. 17, p. 9, http://www.camera.it/544?stenog=/_dati/leg16/lavori/documentiparlamentari/indiceetesti/017/017&pagina=d010#01

78 Cfr. la Relazione annuale 1997, cit., par. 3.2.

79 Tra cui presidenti delle autorità amministrative indipendenti, esperti, rappresentanti dei sindacati e delle imprese, delle associazioni di consumatori, rappresentanti degli enti territoriali, esponenti della magistratura: v. Indagine conoscitiva sulle autorità amministrative indipendenti, cit., 5 s.

governativo, ma prevedano l'intervento di altre qualificate istituzioni o, comunque, la manifestazione di un ampio consenso parlamentare[80]. Applicando tale criterio sembra doversi concludere che le modalità di nomina dei componenti del Garante per la protezione dei dati personali (elezione da parte delle assemblee parlamentari) offrono adeguata garanzia di neutralità rispetto a possibili influenze e condizionamenti esterni.

Non risulta l'esistenza di un dibattito sull'opportunità di introdurre un differente modello di organismo preposto alla tutela della riservatezza dei dati personali.

Risulta dallo studio menzionato in precedenza che non sussistono dubbi circa l'utilità delle autorità amministrative indipendenti, costituite quando un determinato interesse preminente e meritevole di azione pubblica non può essere perseguito pienamente mediante il normale apparato amministrativo pubblico[81].

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	Il Garante è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti eleggono nel loro ambito un presidente ed un vice presidente (art. 153, commi 2 e 3, D.Lgs. 196/2003). Ai sensi dell'art. 3, comma 1, del Regolamento del Garante n. 1/2000, il presidente è eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età. Tale sistema di nomina, che non affida la scelta all'apparato governativo ma che richiede la manifestazione di un ampio consenso parlamentare, costituisce presidio dell'indipendenza dell'autorità.
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	I componenti del Garante sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica. Per tutta la durata dell'incarico essi non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive (art. 153, comma 4, D.Lgs. 196/2003[82]). Il personale di ruolo del Garante deve osservare i divieti e le incompatibilità stabiliti dalle leggi, dai regolamenti e dal codice etico approvato dal Garante (art. 9, Reg. 2/2000; v. art. 6 codice etico[83]).
Ausgestaltung des Arbeitsverhältnisses	I membri dell'Autorità garante per la protezione dei dati personali sono eletti (art. 153 D.Lgs. 196/2003). Essi cessano dalla carica nell'ipotesi di

80 Cfr. l'Indagine conoscitiva sulle autorità amministrative indipendenti, cit., 10, 46.

81 Indagine conoscitiva sulle autorità amministrative indipendenti, cit., 43.

82 L'art. 153, comma 5, precisa che "All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito". V. pure art. 4, commi 1, 2 e 3, Reg. del Garante n. 1/2000.

83 http://www.garanteprivacy.it/web/guest/home/autorita/codice-etico

	dimissioni volontarie, del persistere di una situazione di incompatibilità, per impossibilità a svolgere la propria attività a causa di un impedimento permanente o comunque superiore a sei mesi (art. 4, Reg. 1/2000). Non è regolato il caso di scioglimento per mancato funzionamento. Si presume che una simile decisione possa essere presa solo dalle Camere[84]. Alle dipendenze del Garante è posto l'Ufficio del garante, composto da personale di ruolo. Inoltre, il Garante può assumere, in percentuali minime e a tempo determinato, personale specializzato proveniente dal settore privato (art. 156 D.Lgs. 196/2003). Il trattamento giuridico ed economico del personale del Garante[85] è disciplinato dal Regolamento del Garante n. 2/2000, le cui disposizioni si applicano ai dipendenti di ruolo dell'Autorità, nonché, ove compatibili, al personale collocato fuori ruolo, comandato o distaccato da altre amministrazioni pubbliche o enti pubblici, ovvero assunto con contratto di lavoro a tempo determinato per quanto non previsto da clausole negoziali. Per quanto non previsto dal regolamento stesso si applicano, in quanto compatibili, le disposizioni sullo stato giuridico ed economico dei dipendenti dell'Autorità per le garanzie nelle comunicazioni, e, in via residuale, quelle che disciplinano il rapporto di lavoro privato (art. 2, comma 1). Il vertice dirigenziale dell'Ufficio del Garante è il Segretario generale[86], nominato per la durata del mandato del Garante, egli occupa un posto in ruolo[87].
Zulässigkeit der **Nebenbeschäftigungen**	I membri del Garante, per tutta la durata dell'incarico, non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive (art. 153, comma 4, D.Lgs. 193/2006). Per quanto concerne il personale dipendente, l'art. 9 del codice etico dispone: "1. Il dipendente informa il segretario generale degli eventuali scritti ed articoli che intenda pubblicare nelle materie di competenza del Garante. 2. Ferme restando le disposizioni di cui agli articoli 58 e 58 bis del d.lg. 3 febbraio 1993, n. 29[88] e all'art. 1, commi 56 e seguenti[89], della legge 23 dicembre 1996, n. 662, il dipendente non presta altre attività di lavoro subordinato o autonomo anche di consulenza in materie connesse con quelle di competenza del Garante. 3. Il dipendente non svolge ulteriori attività esterne che contrastano con i doveri o che incidono sul corretto svolgimento dei compiti d'ufficio. Il dipendente dichiara al

84 BUSIA, sub art. 153, in AA.VV., Codice della privacy, T. II, Milano, 2004, 1970 s.

85 L'art. 156, comma 3, D.Lgs. 19672003, rinvia per la disciplina del trattamento giuridico ed economico del personale del Garante per la protezione dei dati personali alla l. n. 249 del 1997, istitutiva dell'Autorità per le garanzie nelle comunicazioni, la quale (art. 1, comma 9), a propria volta rinvia sul punto alla l. n. 481/1995, la quale (art. 2, comma 28) a propria volta – oltre ad escludere l'applicabilità del D.Lgs. 29/1993 – fa rinvio in proposito alla disciplina valevole per l'Autorità garante della concorrenza e del mercato che, infine, a propria volta fa ulteriore e definitivo rinvio (art. 11, comma 2, l. 227/1990) al trattamento previsto per il personale della Banca d'Italia. In definitiva, il Garante stabilisce il trattamento giuridico ed economico del personale con proprio regolamento, da adottarsi in conformità ad una determinata disciplina di riferimento che è – per effetto della suesposta serie di rinvii – quella valevole per il personale della Banca d'Italia.

86 CONTALDO, sub art. 33, in Giannantonio, Losano, Zeno-Zencovich, La tutela dei dati personali, cit., 348.

87 ATELLI, sub art. 156, in AA.VV., Codice della privacy, T. II, Milano, 2004, 2030.

88 V. ora artt. 53 e 54 D.Lgs. 165/2001.

89 Si tratta di disposizioni relative al rapporto di lavoro a tempo parziale.

	segretario generale le situazioni di cui ai commi 2 e 3 del presente articolo anche al fine delle autorizzazioni e comunicazioni previste dalla legge".
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	Non si rinviene alcuna disciplina in ordine al tempo di lavoro dei membri del Garante della privacy.
Länge der Amtsdauer	Il presidente e i componenti dell'Autorità garante per la protezione dei dati personali durano in carica per un mandato di sette anni non rinnovabile.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

I membri dell'Autorità garante per la protezione dei dati personali, per tutta la durata dell'incarico non possono esercitare alcuna altra attività (art. 153, comma 4, D.Lgs. 196/2003).

Alcuni Autori[90] hanno sottolineato che, ad ulteriore garanzia dell'autonomia dei membri del collegio, si potrebbe introdurre una estensione temporale del regime delle incompatibilità per un determinato periodo successivo alla cessazione della carica.

Non si hanno informazioni circa le condizioni di lavoro a tempo pieno o a tempo parziale dei membri del Garante per la protezione dei dati personali.

3.3. Die Entlöhnung insbesondere

Ai sensi dell'art. 153, comma 6, D.Lgs. 196/2003, al presidente dell'Autorità garante per la protezione dei dati personali, compete un'indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente.

Emerge, da uno studio condotto dalla Camera dei deputati, che secondo alcuni presidenti di autorità amministrative indipendenti, sarebbe opportuno che la retribuzione dei membri dei collegi delle autorità fosse omogeneizzata ed eventualmente parametrata sulle retribuzioni più alte riconosciute agli altri organi dell'ordinamento che devono garantire analoga indipendenza, come ad esempio, le alte magistrature[91]. Sembra allora potersi dedurre che l'indennità di funzione riconosciuta ai membri del Garante per la protezione dei dati personali è da considerarsi adeguata.

90 D'ORAZIO, sub art. 30, cit., 306.

91 Cfr. l'Indagine conoscitiva sulle autorità amministrative indipendenti, cit., 17.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	L'indipendenza dell'Autorità garante della privacy, sancita a livello normativo (v. art. 153, comma 1, D.Lgs. 196/2003), è assicurata, tra l'altro, dal fatto che l'elezione dei membri ha luogo interamente in ambito parlamentare, senza coinvolgimento del Governo, né del Presidente della Repubblica. Il numero pari dei componenti del Garante e il voto limitato con cui si eleggono sono elementi volti a garantire la natura bipartisan dell'Autorità di controllo, alla cui composizione concorrono perciò sia le forze di maggioranza sia quelle di opposizione[92].
Möglichkeit der **Weisungen von aussen**	Per le ragioni suesposte si può affermare che la possibilità di influenze esterne è ridotta.
Neutralität der Behörde	La legge disciplina l'Autorità garante in modo da garantirne autonomia e indipendenza. Nondimeno, si è osservato che la tecnica di elezione pervista non garantisce in assoluto dall'influenza di logiche politiche nella scelta dei componenti dell'Autorità. In particolare, il fatto che l'elezione avvenga con voto limitato mira a far sì che anche i candidati delle opposizioni possano entrare a far parte del collegio, la cui composizione è così legata ai rapporti di forza nelle Camere[93].

5. Ressourcen

5.1. Übersicht

Budgethoheit	Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti (art. 156, comma 10, D.Lgs. 196/2003).
Einnahmequellen der Behörde	L'art. 156, comma 3, lett. e, prevede che il Garante definisca, con proprio regolamento[94], la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'art. 6, comma 2, l. 249/1997.
Verfügt die Behörde **über ein eigenes Budget.**	Ulteriore fonte di finanziamento sono costituite dai proventi dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'art. 6, comma 2, l. 249/1997.

5.2. Adäquanz des Budgets insbesondere

Negli ultimi anni si è assistito ad una progressiva, sensibile riduzione del contributo a carico dello Stato. Nella Relazione del Garante del 2011 si legge, tuttavia, che il perseguimento delle finalità

92 PASETTI, Il Garante per la protezione dei dati personali, in MONDUCCI, SARTOR, (a cura di), Il codice in materia di protezione dei dati personali, Padova, 2004, 516.

93 BUSIA, sub art. 153, cit., 1968 s.

94 V. Regolamento n. 3/2000 concernente la gestione amministrativa e la contabilità.

istituzionali è avvenuto nel rispetto degli indirizzi di contenimento della spesa previsti dal legislatore e l'attività amministrativa dell'Autorità non ha subito rallentamenti[95].

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	Ogni individuo ha il diritto di agire per assicurarsi il corretto utilizzo dei dati personali. Ai sensi dell'art. 141 D.Lgs. 196/2003, l'interessato può rivolgersi al Garante: a) mediante **reclamo**, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; b) mediante **segnalazione**, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima; c) mediante **ricorso**, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo. Per interessato si intende la persona fisica cui si riferiscono i dati personali[96].
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	Gli atti che il Garante per la protezione dei dati personali emana nell'esercizio delle sue competenze sono: autorizzazioni (artt. 40 e 41), provvedimenti su reclami, segnalazioni e ricorsi (artt. 143, 144, 150), pareri (art. 153, lett. g), accertamenti (ar. 158) e sanzioni (art. 166).
Weitere Aufgaben der Datenschutzbehörde	No

95 Garante per la protezione dei dati personali, Relazione 2011, in http://www.garanteprivacy.it/documents/10160/2148177/Relazione+annuale+2011.pdf, p. 234.

96 La nozione di interessato è stata modificata dal D.L. 201/2011, convertito in L. 214/2011. Prima delle modifiche, la nozione di interessato era riferibile anche alle persone giuridiche, agli enti e alle associazioni.

6.2. Kompetenzen der Behörde

L'Autorità garante per la protezione dei dati personali si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.

L'organo di vertice, il Collegio svolge funzioni di indirizzo e controllo sul rispetto delle direttive impartite. Alla struttura amministrativa di supporto, l'Ufficio del Garante, competono le funzioni di gestione e di attuazione dei programmi. Il Segretario generale svolge una funzione di raccordo tra la struttura amministrativa e il Garante, essendo assegnatario di compiti sia gestori sia generali di indirizzo e controllo[97].

6.3. Akzeptanz und Ansehen

Non risultano trattazioni specifiche sul tema

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

L'Autorità garante per la protezione dei dati personali non svolge un duplice ruolo.

[97] Cfr. Regolamento n. 1/2000. V. GARRI, sub art. 155, in Aa.Vv., Codice della privacy, cit., 2022 s.

E. Niederlanden

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

1.1. General organization

In articles 53 – 57 of the **Dutch Data Protection Act** ('*Wet bescherming persoonsgegevens*')[98], the rules concerning the conditions and the appointment of the **Data Protection Commission** ('*College bescherming persoonsgegevens*') have been laid down.[99]

In short, the Data Protection Commission (the Commission) comprises **a chairperson and two other members**. They receive remuneration for their work. The term of office and payment of expenses are laid down in general administrative regulations. The chairperson shall be appointed by royal decree, on the proposal of the Ministry of Security and Justice, for six years and the other members for four years. The chairperson and the two other members may not carry out any other remunerated work where the nature of scale of this work is incompatible with the work for the Commission unless they have approval of the Minister. All members can be reappointed immediately after this. In addition, **special members** (who receive a session fee) may be appointed to the Commission. Article 57.2 of the Act states that the members of the Commission shall allocate responsibilities among them and involve the special members therein as much as possible.. Also, article 3 of the Rules of Procedure of the Commission states that the distribution of the tasks of the chairman and the other members of the Commission will be published on the website of the Commission. This has resulted in the so-called **'*mandaatregeling*'**.

There is also an **advisory board** instilled with the task of advising the Commission on general aspects of the protection of personal data. The members of this board must be be drawn from the various sectors of society and must also be appointed by the Minster on the proposal of the Commission. The Commission also has a **secretariat** of which the officials are appointed (an organization consisting of about 70 members of staff), suspended and discharged by the Minister on proposal of the chairperson. The chairperson shall direct the work of the Commission and the secretariat.

1.2. Tasks of the Commission

The framework for performing tasks has been set forth in the Dutch Data Protection Act and other related legislation. In this context, the legislator has implemented Article 28 of the European Data Protection Directive 95/46/EC, which explicitly provides for the existence of such a supervisory authority and which also provides that this **authority should fulfill its task completely independently**. This independence is laid down in article 52.2 Dutch Data Protection Act.

The tasks of the Commission sometimes relate to obligations, but as a rule they relate to powers. Subject to the law and the opinion of the court, the Commission is entitled to take decisions itself regarding the execution of these powers. Other tasks, such as providing information and conducting studies of new developments, result from the general supervisory task. Also in view of its independence, the Commission has considerable freedom to work out the details of its tasks within the frameworks of the Act and to set the necessary priorities and decide where to lay particular emphasis. To this end, article 56 of the Dutch Data Protection Act states that the

---

98 An unofficial English translation of the Dutch Data Protection Act is available at http://www.dutchdpa.nl/Pages/en_wetten_wbp.aspx (14.03.2013).

99 The website of the Data Protection Commission : www.cbpweb.nl (14.03.2013).

Commission shall **adopt rules of procedure** (‘*bestuursreglement*’). These rules must in any case include provisions relating to the financial management and administrative organization of the Commission as well as to working methods and procedures, with a view to a proper and careful discharge of their various tasks. The rules must also provide guarantees against the mixing of the supervisory, advisory and enforcement tasks of the Commission. They may also give more detailed provisions for the advisory board. **The rules themselves and any modifications need to be approved by the Minister of Security and Justice**.

1.3. Powers and competences of the Commission

The Commission **supervises compliance** with Acts that govern the use of personal data. In particular, the Commission supervises compliance with and application of the Dutch Data Protection Act, the Police Data Act and the Municipal Database (Personal Records) Act. Pursuant to the Dutch Data Protection Act, the Commission must be **notified of the processing of personal data**, unless specific processing has been exempted from the notification obligation. If someone fails to notify the Commission of their data processing, the Commission may impose a maximum fine of Euro 4.500. Periodically, the Commission will subject notifications from specific sectors or of specific processing to a further investigation. The Commission will also act upon complaints from data subjects.

In addition to the tasks mentioned above, the Data Protection Act establishes the following tasks: Making recommendations regarding legislation, testing codes of conduct, testing regulations, notification and preliminary examination, information, exemption from the prohibition to process sensitive data, making recommendations regarding permits for transfers to third countries, international affairs, mediation and handling of complaints, official investigation, enforcement, international tasks.

According to article 60 of the Dutch Data Protection Act, the Commission **may initiate an investigation** (on its own or upon request of an interested party) into the manner in which the Act is applied. Provisional findings will be presented to the responsible party as well as to the Minister concerned. In order to carry out such an investigation, members of the Commission are authorized to enter a residence without the consent of the resident. The Commission also has the authorization to apply administrative measures of constraint (article 61 Dutch Data Protection Act).

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	The Dutch Data Protection Act (the Act) sets out the rules on the Data Protection Commission. Article 51 and 52 of the Act state that an Office of the Data Protection Commission has been established with the task to oversee the processing of personal data in accordance with the provisions laid down by and under the Act. The Commission shall also oversee the processing of personal data in the Netherlands, where the processing takes place in accordance with the laws of another country of the European Union. The Commission shall be asked to issue an opinion on bills and draft texts of general administrative regulations relating entirely or substantially to the processing of personal data. Furthermore, the Commission shall perform the other tasks vested in it by law and treat. The Commission is independent in the performance of its tasks (independent governing body, in Dutch: '*zelfstandig bestuursorgaan*'). In this context, the legislator has implemented Article 28 of the European Data Protection Directive 95/46/EC, which explicitly provides for the existence of such a supervisory authority and which also provides that this authority should fulfill its task completely independently. This independence is laid down in article 52.2 of the Act. The Commission falls under the responsibility of the Ministry of Security and Justice.[100] The Commission shall, according to article 56.3 of the Act, adopt rules of procedure ('*bestuursreglement*')[101]. These rules shall in any case include provisions relating to the financial management and administrative organization of the Commission, as well as to working methods and procedures with a view to a proper and careful discharge of its various tasks. The rules shall provide guarantees against the mixing of the supervisory, advisory and enforcement tasks of the Commission. They may also give more detailed provisions for the advisory board.
Organisationsform	The Dutch Data Protection Commission is a commission (independent governing body). All the rules concerning this commission are laid down in the Dutch Data Protection Act or in regulations which can be derived from that Act.
Grösse	The Commission comprises **a chairperson and two other members** (art. 53.1 of the Act). In addition, **special members** may be appointed to the Commission. In the appointment of special members, all efforts shall be made to

100 http://www.rijksbegroting.nl/2013/voorbereiding/begroting?hoofdstuk=40.40 (12.03.2013).

101 The rules of procedure are available on the website of the Commission: http://www.cbpweb.nl/Pages/ind_cbp_bestuur_reglement.aspx (12.03.2013).

	reflect the various sectors of society. The chairperson must fulfill the requirements governing the appointment of District Court judges. There is also an **advisory board** installed with the task to advise the Commission on general aspects of the protection of personal data (art. 53.4 the Act). The Commission also has a **secretariat** (an organization consisting of about 70 members of staff). The chairperson shall direct the work of the Commission and the secretariat.

2.2. Komplexität und Zusammenwirken der Behörden

The Dutch Data Protection Commission is a national commission.

Article 57.2 of the Act states that the members of the Commission shall allocate responsibilities among themselves and shall involve the special members therein as much as possible. Also, article 3 of the Rules of Procedure of the Commission state that the distribution of the tasks of the chairman and the other members of the Commission will be published on the website of the Commission. This has resulted in the so-called '*mandaatregeling*'[102] In the attachment to this Regulation, all the responsibilities and tasks are divided between the chairman and the two members. As a starting point, the chairman is attributed all general responsibilities which are indispensable to the effective performance of the Commission while the two member have separate working fields, not divided by activity (advisory role, decision making, dealing with complaints etc…) but by subject field (e.g. education, employment etc…).

It is stated that the chairman leads the Commission in general, safeguards the progress of it and takes care of implementing the necessary decision-making procedures. He is responsible for institutional affairs including events that are related to the position of the Commission, implementing the tasks of the Commission in accordance with their strategy and plans, drafting policies about the responsibilities of the Commission's members and making sure the policy rules of the Commission are being followed. Also, the chairperson is responsible for external communication, coordinating research projects and managing the two members of the Commission. Besides the foregoing, he must deal with reactions to decisions taken or actions of any other person working for the Commission (e.g. complaints, appeal against a decision) as part of his tasks. Other tasks are coordinating international activities, replacing the two members of the Commissions in their tasks if they are absent at the same time and all other tasks that are not distributed among the two other Commission members.

With respect to the first member of the Commission, his or her tasks are focused on the subject fields of private businesses, international data traffic, technology, employment and social security. The second member has the fields of public administration ('*openbaar bestuur*'), police and justice, education, health and wealth ('*zorg en welzijn*') in their work activities. Both members will replace each other during absence and will also replace the chairperson in urgent situations during his or her absence.

The rule that the chairperson shall direct the work of the Commission and the secretariat is laid down in article 56.2 of the Act.

---

102 In Dutch available on http://www.cbpweb.nl/downloads_mandaatregelingen/mandaatbesluit_voorzitter_leden_regeling_vervanging.pdf (12.03.2013).

The **independence** of the Commission is laid down in article 52.2 of the Act itself: '*The Commission is independent in the performance of its tasks*'. In order to guarantee this independence, the Commission is entitled to take decisions itself regarding the execution of their powers. Other tasks, such as providing information and conducting studies of new developments, result from the general supervisory task. Also in view of its independence, the Commission is free to work out the details of its tasks within the frameworks of the act and to set the necessary priorities and decide where to lay particular emphasis.[103]

In order to avoid conflicts of interest at the Commission, it is stated in article 55.2 of the Act that the chairperson and the two other members may not carry out any other remunerated work where the nature or scale of this work is incompatible with the work for the Commission, without the authorization of the Minister. The possible additional functions of the commissioners are also referred to on the website of the Data Protection Commission in order to promote transparency with regard to any other activities of the commissioners.

In the Netherlands, the Commission is considered to be neutral and independent. The Commission is an independent governing body and, in the execution of its powers, is therefore bound by the standards laid down in the **General Administrative Law Act**. In view of the enforcement powers, the guarantees regarding the proper fulfillment of the tasks have been specified more stringently in the General Administrative Act:

- The possibility of objection to and appeal against the Commission's decisions to the administrative law court.
- The possibility of submitting a complaint to the National Ombudsman**.**
- The Freedom of Information Act (In Dutch: *Wet openbaarheid van bestuur* or *WOB*) applies.
- Pursuant to Article 56.3 the Act, the Commission is obliged to adopt administrative regulations, among other things, providing for rules regarding the work methods and procedures in view of the proper and careful performance of the various tasks.
- As an administrative body, the Commission is of course also bound by the general principles of proper administration.

Also, each year, the Dutch DPA publishes a public annual report explaining its work and findings. Their work is considered transparent since the content is known to the general public. The website of the Dutch Data Protection Authority contains summaries of the annual reports for recent years (article 58 the Act).

No specific information on the advantages and disadvantages of the organization has been revealed by the research.

[103] Based on article 24 of the 'bestuursreglement' the Minister can also instruct priorities, if considered necessary.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	The chairperson of the DPA shall be appointed by royal decree, on the proposal of the Minister of Security and Justice. The two additional 'special' members shall also be appointed by royal decree, on the proposal of the Minister of Security and Justice. The members of the advisory board shall be drawn from the various sectors of society and shall be appointed by the Minster on the proposal of the Commission. The **secretariat** is appointed, suspended and discharged by the Minister on the recommendation of the chairperson.
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	There are no specific rules in this respect.
Ausgestaltung des Arbeitsverhältnisses	Since the Commission is an independent governing body, its member are civil servants.
Zulässigkeit der **Nebenbeschäftigungen**	The chairperson and the two other members may not carry out any other remunerated work where the nature of scale of this work is incompatible with the work for the Dutch Data Protection Authority unless they have approval of the Minister (art. 55.2 the Act).
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	Based on the regulation '*Besluit rechtspositie leden College bescherming persoonsgegevens*', members of the commission can work up to a maximum of 36 hours per week. Upon their own request, the working hours can be amended by the Minister. In this case, the chairperson will be consulted about this request unless it is his own request (article 3a regulation).
Länge der Amtsdauer	The chairperson of the Commission shall be appointed by royal decree for six years and the other members for four years. All members can be reappointed immediately after this. At their own request, the members are discharged by the Minister (art. 53.3 the Act). Members shall in any case be discharged by royal decree on the proposal of the Minister with effect from the first month following the month in which they reach the age of 65 (art. 54.1 the Act). The advisory board is appointed for a period of 4 years. Reappointment can take place twice and for a maximum of 4 years for each reappointment (art. 53.4 the Act).

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

Based on the regulation '*Besluit rechtspositie leden College bescherming persoonsgegevens*', members of the commission can **work up to a maximum of 36 hours per week**. Upon their own request, the working hours can be amended by the Minister. In this case, the chairperson will be consulted about this request unless it is his own request (article 3a regulation). This amendment can be a decrease or increase for the working hours per week (to a maximum of 36 hours).

3.3. Die Entlöhnung insbesondere

Article 55.1 the Act states that the chairperson and the two other members receive remuneration for their work. The special members shall receive a session fee. In all other matters, **their legal position shall be governed by general administrative regulation** ('*Besluit rechtspositie leden College bescherming persoonsgegevens*'). In this regulation, it states in article 4 that the remuneration for the chairman is equal to the remunerations mentioned in attachment A of the so-called **Remuneration decision of the Civil Servants 1984** ('*Bezoldigingsbesluit Burgerlijke Rijksambtenaren*'). This amounts to gross Euro 9.098,26 on a full time basis. For the two members the amount is set in attachment B, remuneration scale 18 which is between gross Euro 6.529,63 to 8.541,18. Article 5 of the regulation '*Besluit rechtspositie leden College bescherming persoonsgegevens*' foresees in a holiday allowance, end-of-year bonus, health costs arrangement and a travel allowance. Also, if the civil servants receive a one-time bonus, the Commission will also receive this. The special members will receive a so-called session fee based on the amount that judges will receive for replacing another judge in court. The chairperson of the advisory board receives an amount of Euro 186,05 per meeting and members of the advisory board receive an amount of Euro 124,79 per meeting (articles 1 and 2 of '*Besluit vacatiegeld Raad van Advies College bescherming persoonsgegevens*').

No documentation has been found confirming whether or not these remuneration models for civil servants are considered reasonable for the members of the Commission.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	Article 52.2 of the Act states: '*The Commission is independent in the performance of its tasks*'. By cause of their appointment by the Minister of Justice, the members of the Commission are independent.
Möglichkeit der **Weisungen von aussen**	In principle, to safeguard their independency, **no instructions can be given to the Commission**. Only the Minister can, based on article 24 of the *bestuursreglement*, set out the framework in which the Commission needs to act. The Minister can also decide that certain efforts on a specific subject of the commission's policy need to be given special attention. The responsibility for a correct fulfillment of their tasks, however, lies with the Commission.
Neutralität der Behörde	Since the Commission is an independent governing body, the Commission should perform **their duties in a neutral way**. They should be impartial and act without prejudice, like all civil servants. Also, as an administrative body, the Commission is of course **also bound by the general principles of proper administration**.

5. Ressourcen

5.1. Übersicht

Budgethoheit	The budget for the Commission is set by the Ministry of Security and Justice. The Commission is an independent governing body and falls under the responsibility of this Ministry (article 24 of the *bestuursregeling*: *The Minister is responsible for financing the Commission*…). **The Commission's budget for 2013 is set at Euro 7.610.000**.[104] In paragraph 5.2 of the '*bestuursreglement*', it is stated that the Commission prepares an estimate for the costs of the Commission's policy for the three following years. This has to take place before 1 August of each year. This estimation needs to be approved by the Minister of Security and Justice. At the same time, the Commission prepares, based on the expected budget, a plan for spending the money for the next year ('*bestedingsplan*'). Also, this plan needs to be approved by the Minister. Before 1 October of each year, the Minister and the Commission discuss these two documents together with the budgets forecasts for the next three years. Before 1 December of each year, the budget is available for the Commission, and the Minister informs the Commission every year before 1 May about the budget for the coming year. Planning for the next several years are mentioned in the estimation of the department of the Ministry of Security and Safety (articles 25-28 *bestuursreglement*).
Einnahmequellen der Behörde	Every year, the chairperson needs to render an account for the finance ('*financiële verantwoording*') of that year. This report needs to contain **an explanation on any difference between the given estimation and the actual costs**, an explanation on the produced results and an explanation on the personnel and formation. This report needs to be offered to the Minister before 15 February of each year and within a timeframe of 30 days, the Minister reacts on this report. Based on this report, the Minister discharges the Commission or requests more information or explanation. If this information or explanation is not satisfactory, there might be consequences for the budget of the coming year (articles 31-33 *bestuursreglement*).
Verfügt die Behörde **über ein eigenes Budget.**	See above.

[104] http://www.rijksbegroting.nl/2013/voorbereiding/begroting,kst173857_23.html.

5.2. Adäquanz des Budgets insbesondere

In the newspaper NRC handelsblad of 15 July 2011, an article was published by Kees Versteegh en Erik van der Walle[105] which led to discussions within the government. The authors of the article, entitled, 'Privacy is hardly guarded, the Commission is restricted and does not act properly' ('*De Privacy wordt nauwelijks bewaakt, College Bescherming Persoonsgegevens mag weinig en doet weinig*'), state that the Commission have few employees (80 full time), few executive powers and a small budget (Euro 7.600.000 per year). This budget can be compared with countries as Italy, Bulgary, Letland and Cyprus. Other countries have a greater budget and more employees. With respect to the powers, critics have said that it is the Commission's own fault, since they focus too much on the legislative aspect of their role and not on informing the people about privacy aspects. This is due to budget cuts in the Commission. Another complaint is that since the Commission have a lot of legally-schooled employees and fewer technical staff, it does not follow the technical developments and is therefore always one step behind. The Scientific Council for Government Policy ('*Wetenschappelijke Raad voor het Regeringsbeleid*')[106] pleaded for a new Commission with more responsibilities, but this was not considered necessary by the government.

In this publication, the authors also requested a reaction of the chairperson of the Commission, Jacob Kohnstamm, about his request to the government to increase the budget for the Commission and the decision of the government to cut the budget by half a million before 2015. His answer is that the Commission already was obliged to cut costs in recent years and that to cut another half million before 2015 will be very difficult; it cannot continue like this with other budget costs.

In reaction to this newspaper article, questions have been asked within the government to the Ministry of Security and Justice. The Ministry of Security and Justice has responded to these questions in a letter of 26 September 2011 by stating that the Commission, in their view, has the same organization and budget as other commissions in other countries. Also after the budget cuts, the personnel and budget should be enough for the Dutch situation. With respect to the budget developments of the last 10 years (from Euro 2.961.000 in 2001 to Euro 7.631.00 in 2011), a huge increase has taken place for the budget of the Commission. At the same time, there have been big technology developments which demand more work for the Commission. As far as the Ministry is concerned, it is of the opinion that these developments in budget and technology have always been well balanced.[107]

---

105 Available free online only through a forum website : http://www.geenstijl.nl/archives/images/collegebeschermingpersoonsgegevens.pdf (14.03.2013).

106 The Scientific Council for Government Policy is an independent advisory body for the Dutch government. Its position is governed by the Act Establishing a Scientific Council on Government Policy of 30 June 1976 ('Instellingswet WRR'). The task of the WRR is to advise the government on issues that are of great importance for society. Unlike other advisory bodies in The Hague, the WRR is not tied to one policy sector. Rather, its reports go beyond individual sectors; they are concerned with the direction of government policy for the longer term. Website of the Scientific Council for Government Policy: http://www.wrr.nl (14.03.2013).

107 A copy of the letter of the Undersecretary of the Ministry of Security and Justice dated 26 September 2011, is available (in Dutch) on: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/09/26/184722-antwoorden-kamervragen-over-kritiek-op-het-college-bescherming-persoonsgegevens-cbp.html

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	The Commission is a governmental, independent organization that deals – amongst other things – with the compliance of the Dutch Data Protection Act as well as the protection of the data subject (according to article 1 of the Act data subject shall mean: '*the person to whom personal data relate'*). By installing a website (in Dutch) called *www.mijnprivacy.nl,* the Commission wanted to inform citizens about all practical questions they might have about this subject. On this website, data subjects can also file a complaint about an organization that does not process the personal data in a proper way, and citizens can request the Commission to mediate in a dispute a data subject might have with an organization. If there is a complaint about the Commission, there is an internal complaint procedure in place and if the data subject is not satisfied with the result of this complaint procedure, the data subject can go to the so-called *Ombudsman* or to Court.
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	Pursuant to the Dutch Data Protection Act, the Commission must be notified of the processing of personal data, unless specific processing has been exempted from the notification obligation. If someone fails to notify the Commission of their data processing, the Commission may impose a fine of up to a maximum of EUR 4,500. A fine can also be imposed if someone has incorrectly or incompletely reported their data processing and/or if they fail to report changes (in time).[108] The notifications have been inserted in to the public registry of notifications (it is a statutory task of the Commission to keep such a register). The public registry provides for openness around the processing of personal data in organizations. This enables a person to check how his or her personal data are being handled, so that he or she can exercise his or her rights, if necessary. In addition, the notifications enable efficient supervision by the Commission. In addition to the tasks mentioned above, the Data Protection Act establishes the following tasks: • Making recommendations regarding legislation (article 51.2) • Testing codes of conduct (article 25) • Testing regulations (article 51.2) • Notification and preliminary examination (article 60) • Information (e.g. article 30) • Exemption from the prohibition to process sensitive data (article 23) • Making recommendations regarding permits for transfers to third countries (article 77.2) • International affairs (e.g article 23.3) • Mediation and handling of complaints (article 47) • Official investigation (articles 31 and 32) • Enforcement (articles 65 through 75)

[108] Based on article 72 Dutch Data Protection Act, the authority to impose a fine lapses five years after the infringement has been committed.

	• International tasks (e.g. article 31.4) According to article 60 of the Dutch Data Protection Act, the Commission may initiate an investigation (of its own volition or upon the request of an interested party) into the manner in which the Act is applied. Provisional findings will be presented to the responsible party as well as to the minister concerned. In order to carry out an investigation, members of the Commission are authorized to enter a residence without the consent of the resident. The Commission also has the authorization to apply administrative measures of constraint (article 61 Dutch Data Protection Act).
Weitere Aufgaben der Datenschutzbehörde	In their work, the decisions and recommendations the Commission always needs to weigh rights of privacy and protecting personal data against the right to information or of free speech or any other human right. The Commission focuses, however, on the rights concerning privacy and personal data. In the Netherlands, the Commission for Human Rights (www.mensenrechten.nl) is in place which is responsible for safeguarding all human rights including freedom of information and freedom of speech etc...

6.2. Kompetenzen der Behörde

As mentioned above, a *bestuursreglement* is in place based on article 56.3 of the Act in which the form of the Commission and their decision making, work processes and organization is worked out. Also a *mandaatregeling* is in place in which the work description of the chairperson and the two members are explained.
Based on article 24 of the *bestuursreglement*, the Minister is responsible for financing the Commission and determines the framework of the commission's policy. The Minister can also decide that certain efforts on a specific subject need explicit attention. As set out in article 14 of the *bestuursreglement*, the Commission - taking into account any advice of the advisory board - drafts a plan for their policy for the next four years ('*beleidsplan*') before 1 December of each calendar year. This plan includes their future activities for the next year and strategic choices for the three years after that.

6.3. Akzeptanz und Ansehen

Not applicable.

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

Not applicable.

F. Polen

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

The supervisory authority for the protection of personal data in Poland is the Inspector General for Personal Data Protection – *Generalny Inspektor Ochrany Danych Osobovych* (Polish abbreviation: GIODO). This one-person authority is appointed by the Sejm of the Republic of Poland (Lower Chamber of the Polish parliament) with the consent of the Senate (Upper Chamber). The term of office of GIODO is 4 years. The same person may hold the office for not more than two terms.

The Inspector General for Personal Data Protection performs its duties assisted by Deputy Inspector General and by the Bureau of the Inspector General for Personal Data Protection. The principles of organisation and functioning of the Bureau are determined in its statute granted by the Regulation of 10 October 2011[109] by the President of the Republic of Poland as regards granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws No. 225, item 1350) and in the organisational rules of procedure. The Bureau is run by the Director who may be appointed and dismissed by the Inspector General.

The Inspector General enjoys legally guaranteed independence - as a non-political authority (the Inspector General may not be a member of any political party or any trade union), she/he may not be removed from the post neither may she/he hold another position except for a professor of a higher education institution. GIODO also enjoys formal immunity.

The Act on the Protection of Personal Data[110] defines tasks of the Inspector General for Personal Data Protection, specifying at the same time the remit of the authority. Pursuant to the wording of Article 12 of the Act, the duties entrusted to the Inspector General comprise, in particular, to supervise the compliance of data processing with the legal provisions on the protection of personal data, to consider complaints and issue administrative decisions ordering the adoption of the proper legal state, to keep the register of data filing systems and provide information on the registered data files, to issue opinions on bills with respect to the protection of personal data, to initiate activities to improve the protection of personal data and to participate in the work of international organisations and institutions involved in personal data protection issues.

To this end, the Inspector General, amongst other things, conducts administrative proceedings in cases connected with compliance with provisions on personal data protection, carries out inspections, addresses the entities concerned with information on malfunctions in data processing, takes part in the reconciliation of legal acts in the scope covered by personal data protection, takes part in works of respective Sejm and Senate commissions, collaborates with domestic and international authorities and organisations dealing with personal data protection and runs educational and informational activity.

In order to ensure effective control over the processing of personal data by the controller, the employees of the GIODO Bureau are entitled to enter premises where the registered data filing systems are being kept, and perform necessary examinations, to demand written or oral explanations, and question any persons responsible for the processing of personal data, to demand

---

109 Rozporzadzenie prezydenta Rzeczypospolitej Polskej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych, http://www.giodo.gov.pl/mwg-internal/de5fs23hu73ds/progress?id=cutryNzCVL <13.03.2013>

110 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883, Dz. U. 2002 r. Nr 101 poz. 926); http://www.giodo.gov.pl/144/id_art/386/j/pl/ <13.03.2013>

the presentation of documents and any data directly related to the subject of the inspection, to demand access to any devices, data carriers and computer systems used for data processing, and to commission expertise and opinions to be prepared.

All of these activities are carried out within the framework of the so-called inspection (audit) in the seat of the controllers. They are obliged to co-operate with the GIODO's inspectors while the inspection is performed, and they are entitled to object to the inspectors' opinions. The material collected during the inspection constitutes the ground for administrative decisions, which are GIODO's most important legal remedy. In case of a breach of provisions on personal data protection, the Inspector General ex officio or on request lodged by a person involved by means of administrative decision orders restoration of the proper legal state, and in particular: a) to remedy the negligence, b) to complete, update, correct, disclose, or not to disclose personal data, c) to apply additional measures protecting the collected personal data, d) to suspend the flow of personal data to a third country, e) to safeguard the data or to transfer them to other subjects, or f) to erase the personal data.

By means of an administrative decision, an order can be made to remedy negligence in the processing of personal data. Past practice was often for most orders to limit the scope of the processed personal data, to use technical and IT means to safeguard the data, to inform the data subjects about the processing conditions, to erase data from the filing system, to suspend certain use of data, to suspend the cross-border flow of data, to obtain the data subject's consent to the processing etc. Decisions issued by the Inspector General are subject to court control. The decisions issued by GIODO may be appealed against with the Voivodship Administrative Court first and then - in the case when the party is not satisfied with the judgment - to the Supreme Administrative Court.111

Apart from the administrative decisions, issuing opinions on the applied legal and technical solutions is an important part of GIODO's activity, as well as issuing opinions and giving answers to the controllers' inquiries. Should the Inspector General find that the activity of a controller bears the attributes of an offence, she/he informs the public prosecutor of the breach of the act on personal data protection. In order to promote the idea of personal data protection, GIODO frequently organises training courses on personal data protection, has her/his own website (www.giodo.gov.pl) and publishes her/his opinions in trade press.

Though each data controller in Poland is obliged to obey the provisions of the act on personal data protection, the GIODO's right to control certain subjects is considerably restrained. GIODO may not control the data processing performed by churches and religious unions with an established legal status, nor may she/he inspect data controllers holding data which constitute a state secret due to the reasons of national security or defence of the state. GIODO, however, may demand explanation from the mentioned controllers, but she/he has no power to issue an administrative decision, if a breach of the law is found. Furthermore, GIODO may not inspect the controllers of data collected by intelligence and counter-intelligence services. The latter is subject to control by the responsible parliamentary committee (also in the field of data protection).

111 On 1 January 2004 provisions of the Act of July 25, 2002 – the Law on the Structure of the Administrative Courts (Journal of Laws No. 153, item 1269) became effective; this act reformed the system of administrative courts covering the Supreme Administrative Court and voivodeship administrative courts. The Supreme Administrative Court carries out the supervision as regards the judgements issued by the voivodeship administrative courts, including the consideration of appeals against the voivodeship administrative courts judgments.

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Independent, monocratic, one-person authority elected by the Parliament (source: The Act on the Protection of Personal Data, Art 8).
Organisationsform	The Inspector General for Personal Data Protection performs its duties assisted by Deputy Inspector General and by the Bureau of the Inspector General for Personal Data Protection. (source: The Act on the Protection of Personal Data and Organisational Regulations of the Bureau of the Inspector General for Personal Data Protection
Grösse	The Inspector General for Personal Data Protection is an independent, monocratic, one-person authority elected by the Parliament with national field of action. The average employment in the Bureau of the Inspector General for Personal Data Protection in 2011 was at the level of 131 regular posts. Among 131 persons employed in the Bureau (this number covers also the Inspector General and his Deputy), 20 persons were employed as auxiliary staff, whereas 111 persons were employed as professional staff. Most of the persons employed in the Bureau have higher education (116), including 76 lawyers and 18 IT technicians.

2.2. Komplexität und Zusammenwirken der Behörden

The duties entrusted to the Inspector General comprise, in particular:

1) supervision over ensuring the compliance of data processing with the provisions on the protection of personal data,
2) issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data,
3) ensuring the obligors' fulfillment of non-pecuniary obligations arising under the decisions referred to in point 2 by the means of enforcement measures foreseen in the Act of 17 June 1966 on enforcement proceedings in administration (Journal of Laws of 2005, no. 229, item 1954 with amendments),
4) keeping the register of data filing systems and providing information on the registered data files,
5) issuing opinions on bills and regulations with respect to the protection of personal data,
6) initiating and undertaking activities to improve the protection of personal data,
7) participating in the work of international organizations and institutions involved in personal data (Article 12 of the Act on the Protection of Personal Data).

The Inspector General performs his/her duties assisted by the Bureau of the Inspector General for Personal Data Protection. Upon a motion of the Inspector General, the Speaker of the Sejm may also appoint a **Deputy Inspector General**. The Deputy Inspector General is dismissed under the same procedure. **The Inspector General determines the scope of tasks of his/her deputy**. The Deputy Inspector General must in principle meet the same requirements as the Inspector General.
The President of the Republic of Poland, having considered the opinion of the Inspector General, can issue a regulation granting a statute to the Bureau and specifying its organization, the principles of its functioning and the seats of **local offices** (at present two: in Katowice and Gdansk) as well as their territorial competence, in order to create optimum organizational conditions for the correct performance of Bureau's tasks.

The Inspector General fulfils its tasks directly or with the assistance of the Director of the Bureau, directors of the Bureau's organisational units and persons indicated in the Bureau's Regulations.

The Bureau ensures performance of the tasks resulting from the responsibilities of the Inspector General specified in the Act and other legal provisions. The Director of the Bureau manages the Bureau with the assistance of directors of particular departments as well as managers of other organisational units. For the organisational structure of the Bureau of the Inspector General for Personal Data Protection, see http://www.giodo.gov.pl/430/j/en/**.**

The Director of the Bureau is responsible for the functioning of the Office, conditions of its functioning and work organisation; he or she also represents the Bureau outside. The duties of the Director of the Bureau include in particular:

1) direct supervision over the Bureau's organisational units,
2) approving documents specifying internal structures of particular organisational units submitted by directors of these units,
3) submitting to the Inspector General applications regarding the number of posts in the Bureau and their division among the Bureau's organisational units,
4) submitting to the Inspector General applications for the positions of directors of particular departments,
5) handling complaints against the Bureau's employees,
6) ensuring compliance with the provisions on state and professional secrecy,
7) submitting to the Inspector General draft rulings, decisions, provisions and certificates,
8) commissioning preparation of evaluations and legal opinions,
9) signing decisions, provisions and certificates under authorisation of the Inspector General,
10) supervising the management of the Bureau's property,
11) supervising public procurement procedures of the Bureau,
12) undertaking financial obligations under authorisation of the Inspector General, within the limits of granted means and according to the rules and procedures specified in the rulings of the Inspector General and in legal provisions,
13) supervising preparation and realisation of the Bureau's budget,
14) collecting property declarations.

The Director of the Bureau is assisted in his work by:

1) **the Secretariat** directly responsible to the Director of the Bureau,
2) **legal counsels** directly responsible to the Director of the Bureau.

The Legal Counsel's tasks include:

1) issuing opinions on draft rulings by the Inspector General,
2) issuing opinions on and initialling draft contracts concluded on behalf of the Bureau,
3) drawing up legal opinions for the purposes of the Bureau's organisational units,
4) acting as attorney ad litem.

The Bureau's statutory organisational units are managed by directors of these units, except for the Finance Department, managed by the Chief Accountant, Independent Position for the Protection of Classified Information, Independent Position for Human Resources and Independent Position for Internal Audit.

The Chief Accountant manages performance of all tasks in the area of the Bureau's budget as well as accounting and financial inspection, according to the principles set forth in separate provisions.

The department's director manages the subordinate department and is responsible for performance of the tasks set forth in the regulations as well as tasks specified by the Inspector General or Deputy Inspector General. The department's director periodically reports on the work of department managed by him or her to the Director of the Bureau. The department's director acts in all cases of the Bureau within the scope of activity of the department managed by him or her. The department's director cooperates with directors of the remaining departments.

Unless provided otherwise in the regulations or other legal provisions, and the handling of a case requires taking **a decision going beyond the responsibilities of the department's director** (and is not possible by means of cooperation of directors of particular departments), the Director of the Bureau, after having asked for their opinions, takes decisions in each case not going beyond the total scope of activities of all his/her subordinate departments. If the handling of a case goes beyond such total scope, the **Director of the Bureau** submits the case to the **Inspector General** or Deputy Inspector General for decision.

At the time of absence of the department's director or his/her deputy, the Director of the Bureau may entrust other employees with his/her substitution. In case of a vacancy at the post of the department's director, the Director of the Bureau may entrust another employee of the Bureau with the fulfilment of these obligations, for a definite time, or take over the management of the department.

The department performs the tasks set forth in the regulations or the **tasks specified by the Inspector General**, Deputy Inspector General or the department's director. The department draws up the draft rulings, decisions, provisions and certificates of the Inspector General as well as draft letters submitted for signing to the Inspector General, Deputy Inspector General or the Director of the Bureau. As necessary, the department agrees on draft rulings, decisions and provisions with other departments. **Persons occupying managerial posts at all levels are responsible** for proper functioning of subordinate organisational units and for performance of other entrusted tasks. The scopes of activity and responsibility for performance of the tasks shall be specified starting with the posts at the lowest level[112].

The department's structure includes:

1) department's director,
2) department's deputy director,
3) department's employees,
4) department's secretariat subordinate directly to the department's director.

If not provided otherwise in the regulations or in the Chancellery Instruction, the scope of activity of the department's secretariat is specified by the department's director. Official activities are performed in accordance with official procedure.

<u>Division of the tasks within the Bureau of the Inspector General for Personal Data Protection</u>

The tasks of the Organisational and Administrative Department include in the main:

[112] The following activities serve the proper performance of tasks by the department's employee: 1) specifying the tasks for particular posts, adequately to the scope of department's activities set forth in the regulations, 2) keeping proper division of responsibilities in the department, 3) cooperation of employees responsible for performance of related tasks, 4) monitoring the performance of tasks, in particular by submitting and accepting periodic reports on work of each organisational unit.

1) providing **organisational services** for the Bureau, including: a) servicing commissions and teams appointed by the Inspector General, b) keeping the Main Chancellery and the Archives, c) keeping a register of all stamps and seals of the Bureau, d) running the Bureau's reporting in the scope typical of the department, e) preparing and keeping records of contracts concluded by the Bureau, f) executing tasks related to occupational health and safety, g) keeping the Central Register of Library Collections;
2) **preparing replies to the Inspector General's addresses** within the scope of the department's activity,
3) **technical support** of business trips and national and foreign delegations,
4) **preparing and conducting public procurement procedures**, and in particular: a) permanent cooperation with the Public Procurement Office, b) examining credibility of economic entities, which can be awarded public procurement contracts, in the scope specified in legal provisions, c) collecting and storing documents connected with public procurement procedure, d) performing other activities concerning public procurement pursuant to universally binding legal provisions as well as activities specified in separate provisions and rulings of the Inspector General;
5) **executing the budget** in accordance with material schedule in cooperation with the Finance Department, including: a) drawing up material schedule to the budget, b) checking invoices and bills in terms of content;
6) **cases related to managing the Bureau**, that is: a) planning and realising purchase of goods as well as outsourcing essential services, b) equipping the Bureau's premises with furniture, devices and other technical means as well as their maintenance, c) managing and keeping records of the Bureau's property, d) insuring the Bureau's property, e) maintenance and current repairs of premises, maintenance of greenery as well as keeping clean premises, green areas, access roads and car parks used by the Bureau, f) organising transport for the purposes of the Bureau, including supervising the work of drivers, g) managing rooms being in possession of the Bureau, h) keeping a storage room.

The tasks of the **Jurisdiction, Legislation and Complaints Department include mainly**:

1) **replying to questions** related to the provisions on personal data protection,
2) **preparing draft addresses** of the Inspector General to public and private sector entities regarding the compliance with the provisions on personal data protection,
3) **drawing up opinions** for the purposes of the Inspector General, Deputy Inspector General and managers of the Bureau's organisational units,
4) **drawing up positions on doctrine and legislation of the Supreme Court**, general and administrative courts, Constitutional Tribunal in cases related to personal data protection,
5) **issuing opinions on bills and regulations** with respect to the protection of personal data,
6) **participating in the work of the commissions and sub commissions of the Government**, Sejm and Senate in connection with handling draft legal acts referred to in point 5 by these authorities,
7) **conducting administrative proceedings** in cases on execution of the provisions on personal data protection,
8) **drawing up draft decisions and provisions** of the Inspector General issued in cases referred to in point 7, and
9) **drawing up draft notifications of commission of crime** and requests for initiating disciplinary proceeding or other proceedings provided for by the law.

The tasks of the **Social Education and International Cooperation Department** include i.a.:

promoting knowledge on personal data protection, including drawing up educational programmes for various target groups, and **organising and executing educational tasks**, including training courses, conferences and seminars, and 3) handling requests for transfer of personal data to third countries.

The tasks of the **Inspection Department** include:

1) conducting, under authorisation of the Inspector General, supervision over **ensuring the compliance of data processing with the provisions on the protection of personal data**,
2) requesting the Inspector General for **authorisation to conduct inspections** and keeping the register of such authorisations,
3) instituting and conducting under the authorisation of the Inspector General **administrative proceedings as a result of irregularities found in the course of the inspection**,
4) **drawing up draft decisions**, provisions and other letters of the Inspector General issued as a result of the inspections conducted, and
5) requesting, on the basis of the findings from the inspection, appropriate proceedings to be instituted against persons responsible for the irregularities which occurred.

The tasks of the **Personal Data Filing Systems Registration Department** include mainly performing tasks connected with **keeping a national, open register of personal data filing systems**, and **performing tasks connected with the provision of information on the filing systems registered**.

The tasks of the **IT Department include i.a.**:

1) cooperating with the Bureau's organisational units as regards **analysis of demand for computer hardware and software** as well as in realisation of purchase of such hardware and software, and in particular: preparation of orders and specifications, analysis of offers in terms of contents as well as technical acceptance,
2) providing the following **services for the Bureau**: a) installing computer hardware and software, b) computer hardware repairs and supervision over use of computer systems, c) managing technical infrastructure of computer systems;
3) **managing computer networks** and systems,
4) providing **ad hoc assistance** to the Bureau's employees as regards the use of computer hardware and software,
5) performing **tasks related to the security of the Bureau's computer systems** and current analysis of the needs in this regard,
6) **drawing up opinions and conducting analyses regarding the processing of personal data** carried on with the use of computer systems for the purposes of the Inspector General, Deputy Inspector General and managers of the Bureau's organisational units, and
7) performing, under authorisation of the Inspector General, **inspection activities along with the employees of the Inspection Department**.

The tasks of the **Finance Department** include:
book-keeping, drawing up the Bureau's draft budget, drawing up reports on budget execution, drawing up the Inspector General's budget execution schedule, drawing up monthly and annual budget reports, analysing the course of the Bureau's budget execution and preparing periodic information in this regard and all other **financial activities** of the Institution.

The tasks of an employee holding the **Independent Position for Human Resources** include i.a. **handling cases related to employing** the Bureau's employees and to their work history, content-related check of payroll, establishing the rights to pensions and pre-retirement benefits, supervising compliance with discipline at work, and keeping a register of rulings issued by the Inspector General.

The tasks of an employee holding the **Independent Position for Internal Audit** include performance of the tasks specified in the Act of 30 June 2005 on Public Finance (Journal of Laws No. 249, item 2104 with later amendments) and the provisions issued on the basis thereof.

The tasks of the Spokesman Team include mainly contact with the media, and drawing up publications for the purposes of the media.

If the number and the character of cases concerning personal data protection in a given area justify it, the Inspector General may perform his tasks with the assistance of local offices of the Bureau (at present two: in Katowice and Gdansk).

The Inspector General for Personal Data Protection is independent, monocratic, one-person authority.

The Act on the Protection of Personal Data and the regulation of activities of the Inspector General for Personal Data Protection were adopted by Polish Parliament as a suitable **political compromise**. There is no evidence of considerable concurring propositions having been presented.

The Inspector General for Personal Data Protection is solely subject to the provisions governed by the Act on the Protection of Personal Data (Art 8(4) of the Act on the Protection of Personal Data).

According to the legal regulation, the Polish Inspector General for Personal Data Protection is considered as independent, impartial and neutral.

No literature or other commentary has been found which discusses this topic.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	The Inspector General is appointed and dismissed by the Sejm of the Republic of Poland with the consent of the Senate (Art. 8(2) of the Act on the Protection of Personal Data).
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	Only a person who meets all of the following requirements may be appointed to the position of the Inspector General: 1) he/she is a Polish citizen permanently residing within the territory of the Republic of Poland, 2) he/she is known for outstanding moral principles, 3) he/she has a degree in law and a proper professional experience, 4) he/she has no criminal record (Art 8 (3) of the Act on the Protection of Personal Data). The Inspector General may neither hold another position (except for a professor of a higher education institution) nor perform any other professional duties. The Inspector General may not be a member of any political party or any trade union, or be involved in any public activity which is not consistent with the integrity of the Inspector General's post (Art. 10 of the Act on the Protection of Personal Data).
Ausgestaltung des Arbeitsverhältnisses	The Inspector General is appointed and dismissed by the Sejm of the Republic of Poland with the consent of the Senate. The Sejm, with the consent of the Senate, can dismiss the Inspector General in the case of: 1) his/her resignation, 2) becoming permanently unable to perform his/her duties due to an illness, 3) violating his/her oath, 4) being sentenced pursuant to a valid court judgment for committing a crime. The Inspector General may neither be held criminally responsible nor deprived of freedom without the prior consent of the Sejm. The Inspector General may not be detained or arrested, except *in flagrante delicto*, and if his/her detention is necessary to secure the due course of proceedings. In such case the Speaker of the Sejm has to be notified of the detention forthwith and may order the detainee to be immediately released. The same rules apply to the Deputy Inspector General
Zulässigkeit der **Nebenbeschäftigungen**	The Inspector General may neither hold another position (except for a professor of a higher education institution) nor perform any other professional duties.
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	The Inspector General may neither hold another position (except for a professor of a higher education institution) nor perform any other professional duties. Position of the Inspector General is considered as a full time job.
Länge der Amtsdauer	The term of office of the Inspector General lasts 4 years following the date of his/her taking the oath. The same person may hold the office of the Inspector General for not more than two terms.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

The position of the Inspector General is considered to be a full time job. Our research has not revealed any further information in this respect. No literature or other commentary which discusses actual or possible side-line work of the employees of **the Bureau of the Inspector General for Personal Data Protection** has been found; according to the annual report of the Institution, all employees' posts are rated as full time roles.

No literature or other commentary has been found on this issue.

3.3. Die Entlöhnung insbesondere

No information.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	With regard to the performance of the duties entrusted to the Inspector General, he/she is solely subject to the provisions governed by the Act (The Act on the Protection of Personal Data Art 8(4).
Möglichkeit der **Weisungen von aussen**	No legal possibility for instructions from outside.
Neutralität der Behörde	The Inspector General may not be a member of any political party or any trade union, nor can he/she be involved in any public activity which is not consistent with the integrity of the Inspector General's post (Art 10 of the Act on the Protection of Personal Data). The Institution is considered as neutral (impartial and independent).

5. Ressourcen

5.1. Übersicht

Budgethoheit	Self-standing accounting item in the Law on State budget adopted by the Parliament
Einnahmequellen der Behörde	The State budget. The Institution applies no charges.
Verfügt die Behörde **über ein eigenes Budget.**	Yes. Independent budget set by the Parliament.

5.2. Adäquanz des Budgets insbesondere

The Organisational Regulations of the Bureau of the Inspector General for Personal Data Protection provide that the Bureau must ensure the performance of the tasks resulting from the responsibilities of the Inspector General as specified in the Act and in other legal provisions and that the scope of the tasks performed by the Bureau is determined by financial resources provided for in the Budget Act. We found no critical (negative) evaluation of this practice:

BUDGET OF GIODO FOR 2009

PART 10
SECTION 751
CHAPTER 75101

in thousand PLN

§	Budget classification paragraph name	**Plan for 2009 r.**
3020	Personnel expenses not being part of remuneration	2
4010	Employee remuneration	8 795
4040	Additional annual remuneration	496
4110	Social insurance contributions	1 250
4120	Labour Fund contributions	226
4170	Supplemental remuneration	10
4210	Materials and equipment purchase	300
4260	Energy purchase	60
4270	Repair services purchase	50
4280	Healthcare services purchase	5
4300	Other services purchase	300
4350	Fees for Internet services	30
4360	Payments for purchase of mobile telephony services	40
4370	Payments for purchase of fixed telephony services	60
4380	Purchase of translation/interpretation services	10
4390	Purchase of services including execution of evaluations, analyses and opinions	5
4400	Rental fees (for office space)	1 440
4410	National business travel	150
4420	Foreign business travel	110
4430	Various payments and contributions	15
4440	Contribution to Company Social Benefit Fund	120
4700	Training courses for employees not being members of civil service	20
4740	Purchase of printing and Xerox copier paper	53
4750	Purchase of computer products, including programmes and licences	100
6060	Expenses for investment purchases	70
In total		**13 717**

Source : http://www.giodo.gov.pl/432/j/en/ 13 717 000 Zł. is approx. 4,1 Million CHF

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	Any party may apply to the Inspector General for reconsidering its case. The decision by the Inspector General on the application to reconsider the case may be appealed against to the administrative court (Article 21 of the Act on the Protection of Personal Data).
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	In order to perform his/her tasks the InspectorGeneral may address state authorities, territorial self-government authorities, as well as state and municipal organizational units, private entities performing public tasks, natural and legal persons, organizational units without legal personality and other entities in order to ensure efficient protection of personal data. The Inspector General may also request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relative to personal data protection. The entity receiving the address or request gives an answer in writing to such address or request within 30 days of its receipt (Article 19a). Once a year the Inspector General submits to the Sejm a report on his/her activities including conclusions with respect to observance of the provisions on personal data protection.
Weitere Aufgaben der Datenschutzbehörde	No other duties.

6.2. Kompetenzen der Behörde

The Inspector General fulfils its tasks directly or with the assistance of the Director of the Bureau, directors of the Bureau's organisational units and persons indicated in the Bureau's Regulations.

The duties entrusted to the **Inspector General** comprise, in particular:

1) supervision over ensuring the compliance of data processing with the provisions on the protection of personal data,
2) issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data,
3) ensuring the obligors' fulfilment of non-pecuniary obligations arising under the decisions referred to in point 2 by the means of enforcement measures foreseen in the Act of 17 June 1966 on enforcement proceedings in administration (Journal of Laws of 2005, no. 229, item 1954 with amendments),
4) keeping the register of data filing systems and providing information on the registered data files,
5) issuing opinions on bills and regulations with respect to the protection of personal data,
6) initiating and undertaking activities to improve the protection of personal data,
7) participating in the work of international organizations and institutions involved in personal data (Article 12 of the Act on the Protection of Personal Data).

In order to carry out these tasks,[113] the Inspector General, the Deputy Inspector General or employees of the Bureau, hereinafter referred to as "the inspectors", authorized by him/her are empowered, in particular to:

1) enter, from 6 a.m. to 10 p.m., upon presentation of a document of personal authorization and service identity card, any premises where the data filing systems are being kept and premises where data are processed outside from the data filing system, and to perform necessary examination or other inspection activities to assess the compliance of the data processing activities with the Act,
2) demand written or oral explanations, and to summon and question any person within the scope necessary to determine the facts of the case,
3) consult any documents and data directly related to the subject of the inspection, and to make a copy of these documents,
4) perform inspection of any devices, data carriers, and computer systems used for data processing,
5) commission expertise and opinions to be prepared (Article 14 of the Act on the Protection of Personal Data).

The head of the unit and any natural person acting as a controller of personal data subject to the inspection are obliged to enable the inspector to perform the inspection functions, and in particular to perform the activities and meet the requirements referred to in the Act on the Protection of Personal Data. The inspector performing the inspection of the data filing systems is authorized to consult any file in which personal data is stored only by means of a duly authorized representative of the unit under inspection. The inspection is carried out upon presentation of a personal authorization form along with a service identity card (Article 15 of the Act on the Protection of Personal Data).

6.3. Akzeptanz und Ansehen

No literature or other commentary has been found which discusses the acceptance of the Institution, but generally, in view of the legal arrangements in place, **the Inspector General for Personal Data Protection** is considered as a respectable office.

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

The Inspector General for Personal Data Protection has no other duties, i.e. the question is not applicable.

---

[113] Especially supervision over ensuring the compliance of data processing with the provisions on the protection of personal data and issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data.

G. Schweden

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

The Data Inspection Board (Datainspektionen) is an autonomous government agency (statlig förvaltningsmyndighet) which falls under / is organized under the Ministry of justice. Such public authority is provided for in the constitution[114] and some basic instructions for how it shall be organized e.g. the management is laid down in an ordinance[115]. Each year, the Government issues general instructions and goals to attain.[116] The Data Inspection Board is not a separate legal entity, but is considered to be a part of the legal entity of the State. However, no public authority, including the Government, may determine how the Data Inspection Board shall, in a particular case relating to the exercise of public authority, make decisions vis-à-vis an individual or a local authority, or relating to the application of law.[117]

The Data Inspection Board has about 40 employees, of whom a majority are jurists, and is led by a Director-General (Generaldirektör). It is organized across five different departments, namely, the Management Team; the Department for matters regarding health care, research and education, the Department for enterprise, the Department for public authorities and working life and the Department for administrative matters.

The Management Team consist of the Director-General, the secretary of the Director General, the General Counsel and the managers of the above mentioned different departments within the Data Inspection Board. The Director-General is appointed by the government for either a limited or non-limited period. The Government can decide to transfer the Director-General to another post within the government administration if it is considered necessary for organizational reasons or if it is considered to be in the interests of the Data Inspection Board itself.[118] The other personnel in the Data Inspection Board (including management) are protected by the general law regarding protection of employment, which provides that there must be objective reasons for dismissal.[119]

The Data Inspection Board has an Insynsråd (Advisory Council) which follows and monitors the work of the Board and gives advices to the Director-General.[120] The Advisory Council has no power to render decisions. The Advisory Council consists currently of six persons from other areas e.g. Members of Parliament, a university professor and director generals from other public authorities. The members of the Advisory Council are appointed by the government. They hold this position as an accessory commission/task and meet normally only a few times per year. Through the Advisory Council the public has insight into the work of the Data Inspection Board.

---

114 Chapter 12 in the Instrument of Government (Regeringsformen), which is part of the Swedish Constitution.

115 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

116 Regleringsbrev för budgetåret 2013 avseende Datainspektionen , available at http://www.esv.se/sv/Verktyg--stod/Statsliggaren/Regleringsbrev/?RBID=14572 (2013-03-11).

117 Chapter 12 Article 2 in the Instrument of Government (Regeringsformen), which is part of the Swedish Constitution.

118 Article 32 and 33 Act (1994:260) on employment in the public sector (Lag (1994:260) om offentlig anställning).

119 See particularly Article 7 and 18 in Lag (1982:80) om anställningsskydd (Employment Protection Act).

120 Article 7 Förordning (2007:975) med instruktion för Datainspektionen (Government ordinance with instruction for the Data Inspection Board).

The Data Inspection Board carries out its work as one unit, and the General-Director is leading this work. The Data Inspection Board's task is to protect the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The Board ensures that authorities, companies, organizations and individuals follow the Personal Data Act, the Debt Recovery Act, the Credit Information Act and the Patient Data Act.[121] The organizational structure of the Board across five different departments reflects the different areas which the Board is supervising in accordance with the above described Acts. The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. It also handles complaints and carries out inspections and renders decisions on matters regarding data protection. By examining government bills, the Board ensures that new laws and ordinances protect personal data in an adequate manner.

An important part of the work of the Board is to provide general information to the public and stakeholders regarding data protection. The Board thus puts significant emphasis on preventive work. Advice and support to personal information representatives (personuppgiftsombud) is prioritized. A personal information representative can be described as an internal auditor in public authorities or companies whose task is to ensure that personal information is handled in a legal manner.

In order to discharge its supervision function, the Board is entitled to obtain on request: access to personal data that is processed; information about and documentation of the processing of personal data and security of this processing; and access to those premises linked to the processing of personal data. If the data is processed in an unlawful manner, the Board renders a decision or an instruction for rectification and can under certain circumstances prohibit (violators being subject to a fine in case of default), the controller of personal data from continuing to process the personal data in any manner other than by storing them. The Board may apply for the erasure of such personal data that has been processed in an unlawful manner at the County Administrative Court. The decisions rendered by the Data Inspection Board can be appealed to the County Administrative Court.[122]

---

121 See http://www.datainspektionen.se/lagar-och-regler/ (2013-03-11) and the legislation there cited.

122 Article 43 to 47 in the Personal Data Act (1998 :204) (Personuppgiftslagen(1998 :204)).

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Autonomous government agency (*statlig förvaltningsmyndighet*) which falls under / is organized under the Ministry of justice. Every year, the Government issues **general instructions and goals** for the Data Inspection Board to attain.[123] Instructions and aims of the Data Inspection Board are also laid down in an ordinance.[124] However, no public authority, including the Government, may determine how the Data Inspection Board shall in a particular case relating to the exercise of public authority make decisions vis-à-vis an individual or a local authority, or relating to the application of law.[125]
Organisationsform	Autonomous government agency (*statlig förvaltningsmyndighet*) which falls under / is organized under the Ministry of Justice. Such public authority is provided for in the Swedish Constitution[126] and some basic instructions for how it shall be organized e.g. the management is laid down in an ordinance.[127] It is considered to be a part of the legal entity of the State, and is therefore not a separate legal entity.
Grösse	There are about 40 employees at the Data Inspection Board organized in to five different departments. The work is led by the Director-General.

2.2. Komplexität und Zusammenwirken der Behörden

The Data Inspection Board is organized and pursues its work on a national level. There are no regional or local authorities or offices.

The Data Inspection Board falls under / is organized under the Ministry of Justice. However, it is an autonomous government agency. The Data Inspection Board‘s mandate and missions are regulated in laws and ordinances enacted by the Government.[128]

The Board independently issues directives and codes of statutes. The Board also renders decisions, handles complaints and carries out inspections. By examining government bills, the Data Inspection Board ensures that new laws and ordinances protect personal data in an adequate manner. These activities are carried out independently and there is no scrutiny by the government or any other public body.

The Director-General is the head of agency of the Data Inspection Board.[129] He is appointed by the Government.

---

123 Regleringsbrev för budgetåret 2013 avseende Datainspektionen , available at http://www.esv.se/sv/Verktyg--stod/Statsliggaren/Regleringsbrev/?RBID=14572 (2013-03-11).

124 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

125 Chapter 12 Article 2 in the Instrument of Government (Regeringsformen).

126 Chapter 12 in the Instrument of Government (Regeringsformen).

127 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

128 See particularly Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

The Data Inspection Board has an **Advisory Council** (*Insynsråd*) which follows and monitors the work of the Board and gives advices to the Director-General.[130] The Advisory Council has no power to render decisions. The members of the Advisory Council are appointed by the government. They hold this position as an accessory commission/task and meet normally only a few times per year. Through the Advisory Counci,l the public has insight in to the work of the Data Inspection Board.

The Data Inspection Board is organized in the same way as most Swedish public authorities that fall under the Government. It has been organized in accordance with this general organization scheme since it was created in 1973.

The independence of the Data Inspection Board is provided for in law in such a way that no public authority, including the Parliament, or a decision-making body of any local authority, may determine how it shall adjudicate in a particular case relating to the exercise of public authority vis-à-vis an individual or a local authority, or relating to the application of law.[131] Moreover, the Board itself issues directives and codes of statutes regarding data protection issues.[132]

The Data Inspection Board has not been subject to any considerable criticism from major stakeholders that the Board is not neutral or that it is affected by particular political interests. In comparison with other public authorities, the Data Inspection Board enjoys a high level of confidence from the public.[133]

There does not appear to have been any significant debate regarding the disadvantages and advantages of the organizational structure.[134] However, some stakeholders have argued that they should be more involved in the development of the Data Inspection Board's directives and codes of statutes, suggesting that these regulations should be developed to a greater extent through consultation with the affected industry.[135]

---

129 Article 5 and 7 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

130 Article 7 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

131 Chapter 12 Article 2 in the Instrument of Government (Regeringsformen).

132 The mandate for an administrative authority such as the Data Inspection Board to issue regulations and general advice is provided for in chapter 8 in the Instrument of Government (Regeringsformen). Such a mandate is dependent on the delegation of power from the Government by an ordinance.

133 See e.g. Motion 2009/10:K422 Datainspektionen and Motion 2011/12:K338 Personnummer och personlig integritet (Suggestion from Members of Parliament to raise the budget of the Data Inspection Board and to give the Board extended power e.g. regarding the possibility to issue fines in case of violation of data protection laws and regulations).

134 A probable conclusion regarding this lack of discussion is that the Data Inspection Board and major stakeholders are content, or at least not discontent, with the organizational scheme of the Board.

135 Regeringens proposition 1993/94:116 p. 12.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	The government appoints the Director-General and the members of the Advisory Council. Appointments to other posts are made by the Data Inspection Board itself (a government ordinance designates the Board to carry out this task).[136]
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	Only objective factors, such as merit and competence, shall be taken into account when appointing personnel to posts at the Data Inspection Board. There are no formal requirements to be fulfilled. This concerns both the Director-General, the members of the Advisory Council and other staff.[137]
Ausgestaltung des Arbeitsverhältnisses	The Director-General is considered as a staff member in a leading position (verksledande ställning). The Government can decide to transfer the Director-General to another post within the Government administration if it is considered necessary for organizational reasons or if it is considered to be in the interest of the Data Inspection Board itself.[138] The other personnel at the Data Inspection Board (including management) are civil servants and are protected by the general law regarding protection of employment, which provides that there must be objective reasons for dismissal.[139]
Zulässigkeit der **Nebenbeschäftigungen**	An employee can pursue secondary employment/activity as long as it does not undermine the confidence in his or any other employee's impartiality nor harm the reputation of the Data Inspection Board.[140]
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	There are no regulations on full or part time work at the top management level.
Länge der Amtsdauer	The Director-General can be appointed for a limited period. If this is the case, the length of that period is decided by the Government. There is no limit for how many times the Director-General can be re-elected.[141] Other personnel in the Management team are appointed on a permanent basis. The members of the Advisory Council are elected by the Government for a limited period, in general, three years.[142]

136 See chapter 12 Article 5 in the Instrument of Government (Regeringsformen) and Article 22 and 23 Ordinance for autonomous government agency(2007:515) (Myndighetsförordning (2007:515)).

137 Chapter 12 Article 5 in the Instrument of Government (Regeringsformen).

138 Article 32 and 33 Act (1994:260) on employment in the public sector (Lag (1994:260) om offentlig anställning).

139 See particularly Article 7 and 18 in Lag (1982:80) Employment Protection Act (Lag (1982:80) om anställningsskydd).

140 Article 7 Act (1994:260) on employment in the public sector (Lag (1994:260) om offentlig anställning).

141 See Article 42(3) Act (1994:260) on employment in the public sector (Lag (1994:260) om offentlig anställning) and Article 9 Government ordinance on public employment (1994:373) (Anställningsförordning (1994:373)).

142 See Article 6 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen) and Ledamot av insynsråd (Government guideline), Finansdepartementet, January 2008, p. 4.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

There seem to be no literature regarding the Data Inspection Board in particular. However, there is literature which in more general terms concerns secondary employment/activity of civil servants and officials. Such secondary employment/activity is acceptable so long as it does not undermine the confidence in the civil servant‘s or the official‘s impartiality or harm the reputation of the public authority. Activities that are normally not prohibited are commissions of trust regarding trade unions, political parties, non-profit associations and commissions of trust from Government and regional governments in general.[143]

The Director-General works full time. There is no information to be found regarding the other personnel in the management team. The members of the advisory council to the Director-General hold this position as an accessory commission/task and normally attend meetings only a few times per year.

3.3. Die Entlöhnung insbesondere

No information concerning the Data Inspection Board in particular can be found in this regard. However, the general view is that Director-Generals of autonomous government agencies such as the Data Inspection Board are relatively well remunerated.

[143] E. Hinn, Kommentar i Karnov till 7 § Lag (1994 : 260) om offentlig anställning.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	The Government can decide to transfer the Director-General to another post within the government administration if it is considered necessary for organizational reasons or if it is considered to be in the interests of the Data Inspection Board itself.[144] The Director-General thus needs to have the support of the government. The other personnel in the Data Inspection Board (including management) are protected by the general law regarding protection of employment, which provides that there must be objective reasons for dismissal.[145]
Möglichkeit der **Weisungen von aussen**	Each year, the Government issues general instructions and goals for the Data Inspection Board to attain. However, no public authority, including the Parliament and Government, may determine how the Data Inspection Board shall, in a particular case, make decisions relating to the exercise of public authority vis-à-vis an individual or a local authority, or relating to the application of law.[146]
Neutralität der Behörde	The Data Inspection Board is neutral to the extent that it is not controlled nor needs to consider instructions/requests originating from particular political interests or other stakeholders; it must only comply with general instructions from the government. The Director-General represents the Data Inspection Board. However, as discussed above, he needs the support of the government to maintain his position. The members of the Advisory Council represent the public, rather than any particular political interests.[147]

144 Article 32 and 33 Act (1994:260) on employment in the public sector (Lag (1994:260) om offentlig anställning).

145 See in particular Article 7 and 18 Employment Protection Act (1982:80) (Lag (1982:80) om anställningsskydd).

146 Chapter 12 Article 2 in the Instrument of Government (Regeringsformen).

147 Ledamot av insynsråd (Government guidelines), Finansdepartementet, January 2008, p. 3.

5. Ressourcen

5.1. Übersicht

Budgethoheit	The overall budget is decided each year by the Government. There is no parliamentary scrutiny of the budget. For 2013, the budget is set at about 42 million Swedish crowns.[148]
Einnahmequellen der Behörde	The Data Inspection Board can charge a fee for goods and services provided to the public with an amount corresponding to 10 per cent of the total costs for the Board's activity in this regard.[149]
Verfügt die Behörde **über ein eigenes Budget.**	Yes

5.2. Adäquanz des Budgets insbesondere

It has been argued by Members of Parliament that the budget should be increased in view of the important and increasingly complex task of the Data Inspection Board.[150]

148 Regleringsbrev för budgetåret 2013 avseende Datainspektionen p. 3, available at http://www.esv.se/sv/Verktyg--stod/Statsliggaren/Regleringsbrev/?RBID=14572 (2013-03-11).

149 Regleringsbrev för budgetåret 2013 avseende Datainspektionen p. 3, available at http://www.esv.se/sv/Verktyg--stod/Statsliggaren/Regleringsbrev/?RBID=14572 (2013-03-11).

150 Motion 2009/10:K422 Datainspektionen (Suggestion from members of parliament to raise the budget of the Data Inspection Board).

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	Individuals can make a request / file a complaint at the Data Inspection Board. Such request can lead to an inspection. A complaining party always receives an answer from the Board. The Board puts significant emphasis on preventative work, principally by providing information. Advice and support to personal information representatives (personuppgiftsombud) is prioritized. Personal information representatives can be described as internal auditors in public authorities and companies whose task is to ensure that personal information is handled in a legal manner.
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	The Data Inspection Board issues directives and codes of statutes and renders decisions on matters regarding data protection.[151] To discharge its supervision duties, the Board is entitled to obtain the following on request: access to personal data that is processed; information and documentation about the processing of personal data and security of this data processing; and access to those premises linked to the processing of personal data.[152] If the data is processed in an unlawful manner, the Board renders a decision or an instruction for rectification and can under certain circumstances prohibit (enforced by the possibility of a fine in case of default) the controller of personal data from continuing to process the personal data in any manner other than by storing them.[153] The Board may apply to the County Administrative Court for the erasure of such personal data that has been processed in an unlawful manner.[154]
Weitere Aufgaben der Datenschutzbehörde	The Data Inspection Board's mandate only concerns the supervision of protection of data.

6.2. Kompetenzen der Behörde

The Data Inspection Board's task is to protect individuals' privacy in an information society without unnecessarily preventing or complicating the use of new technology. The Board ensures that authorities, companies, organizations and individuals comply with the Personal Data Act, the Debt Recovery Act, the Credit Information Act and the Patient Data Act.[155] The Board works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. The Board also handles complaints, carries out inspections and renders decisions. The core activity of the Board is supervision under the Personal Data Act. The Board has aimed to use one third of its resources (according to the number of hours devoted by its personnel) on its inspection duties under the above cited laws and another third of the resources for the provision of information to the public and the development of directives and codes of statutes.[156] Advice and support to personal information representatives (personuppgiftsombud) is prioritized. As discussed above, personal information representatives can be described as internal auditors in public authorities and

151 Article 50 and 51 Personal Data Act (1998 :204).

152 Article 43 Personal Data Act (1998 :204).

153 Article 45 Personal Data Act (1998 :204).

154 Article 47 Personal Data Act (1998 :204).

155 See http://www.datainspektionen.se/lagar-och-regler/ (2013-03-12) which refers to relevant laws.

156 SOU 2002 :2, Bilaga 5, p. 265.

companies whose task it is to ensure that personal information is handled in a legal manner. The rest of the resources are used for all remaining activities of the Board, e.g. administrative work.

The Board works as one unit and the Director-General leads this work. The Board's decisions and guidelines are rendered, adopted and signed by the Director-General. The Advisory Council has no power to render decisions. Its only mission is to monitor the work of the Board and to give advice to the Director-General.[157] The organizational structure of the Board across the Department for matters regarding health care, research and education, the Department for enterprise and the Department for public authorities and working life reflects the different areas which the Board supervises in accordance with the above described Acts.

6.3. Akzeptanz und Ansehen

There is no literature concerning this matter. However, since the Data Inspection Board's aim is to protect individuals, it has been emphasized that it is important that it enjoys a high level of confidence from the public and the media.[158] It has been stated that the Board enjoys such a high level of confidence in comparison to other public authorities.[159]

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

The Data Inspection Board is responsible for data protection, not for the freedom of information. There are therefore no double roles.

---

157 Article 7 Government ordinance (2007:975) with instruction for the Data Inspection Board (Förordning (2007:975) med instruktion för Datainspektionen).

158 SOU 2002:2, p. 160.

159 See e.g. Motion 2009/10:K422 Datainspektionen and Motion 2011/12:K338 Personnummer och personlig integritet (Suggestion from Members of Parliament to raise the budget of the Data Inspection Board and to give the Board extended powers e.g. regarding the possibility to issue fines in case of violation of data protection laws and regulations).

H. Das Vereinigte Königreich

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

The Information Commissioner's Office (**ICO**)[160] is the UK's independent public authority set up to uphold information rights. Previously known as the Data Protection Registrar, and then the Data Protection Commissioner, the role was revised in January 2002, incorporating additional duties under the Freedom of Information Act 2000 (**FOIA 2000**), and renaming the position to Information Commissioner.

Under the Data Protection Act 1998 (the **DPA 1998**), the **Information Commissioner** him or her-self is an independent person appointed by the Queen with responsibility for setting the priorities of the ICO. The ICO is considered to be an independent Non-Departmental Public Body, sponsored by the relevant Government department, the Ministry of Justice. Its budget for 2012/13 is £19,695,100.[161]

The ICO has specific **regulatory powers** as well as a broad remit **to educate and inform** the public about data protection. The ICO's main responsibilities are to enforce and oversee the DPA 1998, the FOIA 2000, the Environmental Regulations 2004 and the Privacy and Electronic Communications Regulations. Supported by a body of **approximately 350 staff** at the ICO, the main functions of the Commissioner are to educate and influence practice relating to data protection, to resolve complaints from those who consider their rights have been breached and to enforce regulations set out in the above legislation.

The **DPA 1998** allows individuals access to personal information held on them, by both public authorities and private organisations, and requires all organisations that process such data to comply with **eight principles**, making sure that personal information is: fairly and lawfully processed, processed for limited purposes, adequate, relevant and not excessive, accurate and up to date, not kept for longer than is necessary, processed in line with that person's rights, secure and not transferred to other countries without adequate protection. All organisations which process such data are required to notify the Information Commissioner who enters their details on a public register. There are currently 355,292 organisations which have notified with the ICO.

The **data protection powers** of the Information Commissioner include: conducting **assessments** to check that organisations are complying with the DPA 1998, to **serve information notices** requiring organisations to provide the ICO with specified information within a certain time period, to serve **enforcement notices** requiring organisations to take specified steps to ensure they comply with the law, to prosecute those who commit criminal offences under the DPA 1998, to **conduct audits** for determining whether good practice is being followed and to **report to Parliament** on data protection issues of concern. For the period 2011/12, 12,985 cases were received, while 12,725 cases were closed. Insofar as enforcement is concerned, only two enforcement notices were issued, while 15 prosecutions were pursued and 10 civil monetary penalties were handed down. 42 audits were carried out.

The **FOIA 2000**, implemented in January 2005, gives people the general right of **access to information held by over 100,000 public authorities** in the UK. The Information Commissioner is responsible for guidance on set procedures for responding to requests. The ICO will receive

---

160 This term is commonly used interchangeably with "The Information Commissioner".

161 All figures obtained from ICO document, Key Facts 2011/2012, available at http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx (05.03.2013).

complaints about public authorities' conduct of their responsibilities, and after investigation, the ICO will make a final assessment as to whether or not the relevant public authority has complied with the FOIA 2000. **Enforcement action** may be taken against public authorities that repeatedly fail to meet their responsibilities under the FOIA 2000. In the period 2011/2012, 4,633 cases were received, while 4,763 were closed.

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Under section 6(2) DPA 1998, the Information Commissioner is **appointed by the Queen** using Letters Patent[162] (on advice from the Prime Minister, who is in turn, advised by the Secretary of State for Justice following a selection process undertaken by his Department, validated by the Office of the Commissioner for Public Appointments and scrutiny by the House of Commons Justice Committee, a committee of cross-party Members of Parliament from the UK's lower house of representatives). He or she is **not a civil servant but is an independent official answerable directly to Parliament**. He or she is not answerable to a Government Minister, and exercises legal powers which are vested directly in him and are not delegated from a Minister.
Organisationsform	The Information Commissioner has **legal personality as a 'corporation sole'**.[163] This is a little used form of corporate personality employed where powers and responsibilities are vested in an individual office-holder. The usual example of a corporation sole is of a bishop. The ICO which supports the Commissioner in his work, is a **non-departmental public body** sponsored by the Ministry of Justice. Although the Commissioner operates independently in the exercise of his statutory functions, some issues require the approval of the Secretary of State, such as funding.
Grösse	The ICO is staffed by approximately **350 staff** across five separate office locations. In discharging his statutory responsibilities, the Information Commissioner is principally assisted by a Management Board consisting of the Executive Team and four Non-Executive Directors. The Executive Team is made up of the Information Commissioner, the Director of Operations, the Director of Corporate Services, the Deputy Commissioner with responsibility for Data Protection supervisory functions and the Deputy Commissioner with responsibility for Freedom of Information. The Management Board oversees the work of four other teams and committees, including the Audit Committee and Executive Team.

162 Letters patent are a type of legal instrument in the form of a published written order issued by a monarch president, generally granting an office, right, monopoly, title, or status to a person or corporation.

163 Schedule 5, Part I, section 1(1).

2.2. Komplexität und Zusammenwirken der Behörden

The ICO is a national organisation, with its main office in Wilmslow, Cheshire and another office in London. There are however **three regional offices**, which fall under the responsibility of the Director of Operations, namely, the Northern Ireland office, the Scotland office and the Wales office. Their functions are described as providing a local point of contact for members of the public and organisations based in their respective regions. As well as operating an advice service to address general enquiries on data protection and freedom of information, they each respectively promote good practice in information rights by raising awareness of organisational responsibilities across all sectors. They also influence policy in related areas by working closely with the departments of their regional administrations and the wider public sector.

The respective responsibilities of the Ministry of Justice and the Information Commissioner are set out in a **Framework Agreement**,[164] the latest version of which has been effective since September 2011. This clarifies that, as set out in the DPA 1998, the Information Commissioner must be completely independent of Government, yet at the same time is accountable to Parliament for the exercise of his statutory functions.

The **duties of the Information Commissioner** insofar as the Ministry of Justice are concerned are various, ranging from the provision of annual reports and accounts, making arrangements for audits, and developing corporate and business plans. The **Ministry of Justice** on the other hand, is, among other things, responsible for ensuring that the Secretary of State for Justice will answer for the ICO in Parliament and for answering Parliamentary Questions relating to the ICO. The Agreement also regulates funding arrangements for the ICO, and in accordance with the DPA 1998,[165] the Secretary of State retains responsibility for making payments (known as 'grant in aid') to the ICO out of money provided by Parliament.

There are **no particular regulations concerning the responsibilities and/or skills** of those with key responsibilities in the ICO. A **Job Description**[166] was nevertheless formulated for the most recent selection process for an Information Commissioner undertaken by the Ministry of Justice in 2009; this states that the Information Commissioner is responsible for: the fulfilment of all the statutory responsibilities conferred upon him; providing leadership and strategic direction for the Commissioner's office, building and maintaining excellent personal and organisational relationships with key stakeholders, including Ministers, Parliament, the media, public interest groups, business and international equivalents; contributing to debates on the development of policy, nationally and internationally, on data protection and freedom of information issues, and acting as Accounting Officer for the Commissioner's office. The Person Specification demands skills in the areas of leadership, communication, intellect, judgment and experience and personal qualities.

The DPA 1998[167] prescribes only that the Commissioner appoint a deputy commissioner, or two deputy commissioners, and furthermore, that he may appoint such number of other officers and staff as he may determine. The Commissioner is also required, when appointing any second deputy

---

164 Ministry of Justice and ICO, Framework Agreement, September 2011, available at http://www.ico.gov.uk/about_us/how_we_work/~/media/documents/library/Corporate/Research_and_reports/framework_agreement_moj_ico.ashx (05.03.2013).

165 Schedule 5, Part I, sections 8 and 9.

166 See Annex B of House of Commons Justice Committee, The work of the Information Commissioner: appointment of a new Commissioner, Third Report of Session 2008-09, February 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmselect/cmjust/146/146.pdf (05.03.2013).

167 Schedule 5, Part I, Section 4.

commissioner, to specify which of the Commissioner's functions are to be performed by the deputy commissioner. These functions are left to the discretion of the Commissioner.

This particular organisational structure is considered to allow the ICO to discharge its functions as a regulator. The origins of the ICO lie in the **Data Protection Act 1984**, which introduced the eight principles of good practice for the handling of data. For the first time, data users – those persons who held data – were obliged to register with a supervisory authority – at this time, the Data Protection Registrar. In 1995, **EU Directive, 95/46/EC** was adopted, requiring all Member States to pass national legislation giving effect to the legislation. This obliged each Member State to set up a supervisory authority to oversee the application in its own country of the national provisions giving effect to the Directive. The **DPA 1998 replaced the 1984 regime**, and implemented the Directive in the UK, taking data protection to a new level of complexity. Following implementation of the DPA 1998 in March 2000, the title of the office was changed to Data Protection Commissioner.

Subsequently, in addition to being the regulator for Data Protection legislation, the ICO's functions were extended after implementation of the FOIA in 2000 to regulate Freedom of Information, and the titled changed to Information Commissioner.

The position of the Government[168] is that it wants an independent and influential ICO. The present structure and relationship with Government as governed by the Framework Agreement is said to further the ICO's financial and administrative independence, balanced with appropriate reporting arrangements to enable the Ministry of Justice to maintain and ensure the proper expenditure of public money allocated to the ICO.

Measures to better ensure the independence of the ICO are set out in more detail in section 4 below, but include:

- **Legislative underpinning of the Information Commissioner**, confirming that he or she is not a civil servant but reports directly to Parliament, including the Annual Report;
- The **Framework Agreement** which sets out the respective responsibilities of the Ministry of Justice and the Information Commissioner to support the work of both organisations and to ensure propriety and value for money;
- The recent **Protection of Freedoms Act 2012** has now introduced further measures to enhance the Commissioner's independence, including no longer needing to seek consent of the Justice Secretary on issues relating to staff appointments, charging for certain services or before issuing certain statutory codes of practice under the DPA 1998;
- The Commissioner is **supported by his Management Board** which provides oversight for the Commissioner and the ICO;
- Decision making is also overseen by four **Non-Executive directors**;
- The Management Board is supported by an **Audit Committee** which provides scrutiny, oversight and assurance on risk control and government procedures;
- The **Remuneration Committee** considers and advises the Commissioner and his Management Board on the ICO's remuneration policies and practices;

168 See Ministerial Statement of Lord McNally, available at http://www.theyworkforyou.com/wms/?id=2011-09-15a.68.0 (06.03.2013).

- The **appointments process** of the Commissioner is subject to validation by a Commissioner for Public Appointments and vetting by the House of Commons Justice Committee;[169]
- The **Information Tribunal**, consisting of a legally qualified chairman and deputies hears appeals against the service of any enforcement and information notices issued by the ICO;
- **Internal ICO policies** include a Code of Conduct, as well as rules on the acceptance of gifts, the publicly available registers of interests and a code of conduct, further enhancing transparency and independence of the ICO as a whole.

From a cursory review of political debate and other commentary on the performance of the ICO, the Commissioner and the ICO as a regulator are **widely viewed as impartial and apolitical**. Criticisms uncovered are largely confined to the ICO's efficiency in the way that it performs its duties rather than any suggestions that it is in any way politically biased.

Debate in the UK in recent years insofar as the organisation of the ICO and its relationship with government is concerned appears to centre on two issues.

First, successive parliamentary committees,[170] principally the House of Commons Justice Committee, have called for the Information Commissioner to become **directly responsible to, and funded by, Parliament** rather than continuing to owe obligations to the Ministry of Justice. The most recent House of Commons Justice Committee Report on this issue recommended that the Information Commissioner become directly responsible to, and funded by, Parliament, after hearing evidence from the current Information Commissioner that the ICO could be viewed simply as a branch of Government.[171]
The Government, in its Response,[172] rejected the Recommendation, arguing that the Framework Agreement and Protection of Freedoms Act 2012 (see above) deliver a real enhancement to the ICO's corporate and administrative independence, and that the ICO should not become a parliamentary body as its functions do not primarily relate to the business of Parliament. It further claims that Parliament already exercises considerable oversight of the ICO and that the role of Parliament in the scrutiny of the appointment of the Commissioner has already been enhanced.

Secondly, the **constitution of the Information Commissioner** has been addressed in several occasions, most notably at the House of Commons Justice Committee hearing which considered the

---

169 The Government has since announced that it will offer the House of Commons Justice a pre-appointment hearing with the Government's preferred candidate for Information Commissioner and will accept the committee's conclusion on whether or not the candidate should be appointed – see statement of Minister of State at http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/110216-wms0001.htm (06.03.2013).

170 See also the Government Response to the recommendation of the Constitutional Affairs Select Committee Report in 'Freedom of Information – one year on' (October 2006), where the Government rejected the proposal of the Information Commissioner being directly responsible to, and funded by Parliament, available at http://www.official-documents.gov.uk/document/cm69/6937/6937.pdf (11.03.2013).

171 Evidence of Christopher Graham, Information Commissioner, to House of Commons Justice Committee for Ninth Report of Session 2010-12: Referral fees and the theft of personal data, available at http://www.publications.parliament.uk/pa/cm201012/cmselect/cmjust/1473/147304.htm#a4 (06.03.2012).

172 Government Response to the House of Commons Justice Committee for Ninth Report of Session 2010-12: Referral fees and the theft of personal data, Recommendation 4, available at http://www.official-documents.gov.uk/document/cm82/8240/8240.pdf (06.03.2013).

appointment of the current Information Commissioner.[173] In particular, there is a concern that there is the potential for confusion in the status of statements coming from the organisation, the ICO, and those issued explicitly by the Commissioner. The previous Information Commissioner, Richard Thomas, had recommended[174] that the Information Commissioner's role should be undertaken by a multi-member 'Information Commission' to strengthen the influence and authority of the ICO, to de-personalise relations between regulator and key stakeholders, to reduce risks of inappropriate pressure from such stakeholders, to reduce the risk of a maverick appointment and to draw in a diversity of background and skills.

The Committee however agreed with the view of the current Information Commissioner that the Information Commissioner remain as a commissioner rather than a multi-member commission. Certain responsibilities, it was noted, such as the task of personally reading the controversial material of Cabinet minutes (i.e., minutes of the meetings of UK Government Ministers) on the decision to invade Iraq in 2003, following a freedom of information request, are responsibilities not appropriate for a multi-member commission. The House of Commons Justice Committee concluded that the personal responsibility of the Information Commissioner for the regulation of data protection and freedom of information is the main value of the way in which the role is constituted, and that it is important that the branding of communications from the ICO leaves no room for confusion about the personal responsibility of the Commissioner.[175]

---

173 House of Commons Justice Committee, The Work of the Information Commissioner, Op. cit., paras. 26-28

174 In R. Thomas and M. Walport, the Data Sharing Review Report (11 July 2008), para. 8.74 available at http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf (06.03.2013).

175 House of Commons Justice Committee, The Work of the Information Commissioner, Op. cit., para 28.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	Section 6(2) of the DPA 1998 prescribes that the **Information Commissioner is appointed by the Queen** by Letters Patent (see section 2 above). The Information Commissioner has sole responsibility for appointing **one or two deputy commissioners, and other officers and staff** may be appointed as the Commissioner may determine. As to the **appointment process of the Commissioner**, until October last year, the Queen acted on advice from the Prime Minister, who, in turn, was advised by the Secretary of State for Justice following a selection process undertaken by his Department – validated by the Office for the Commissioner for Public Appointments and scrutiny by the House of Commons Justice Committee. For all future appointments, the Protection of Freedoms Act 2012[176] amends the DPA 1998 to clarify that no recommendation may be made to the Queen for the appointment of a person as the Commissioner unless the person concerned has been **selected on merit on the basis of fair and open competition**. The Government has clarified that the House of Commons Justice Committee will be entitled to a pre-appointment hearing with the preferred candidate and will accept the committee's conclusion on whether or not the candidate should be appointed.
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	The ICO operates a **Code of Conduct**,[177] as recommended for all non-departmental public bodies by the Committee on Standards in Public Life.[178] This has no legal force, but does form part of staff members' terms and conditions of service. It contains provisions on conflicts of interest, integrity, relations with the public, effective use of resources, official information and staff concerns about improper conduct. The ICO has a **Register of Interests**[179] which is to be completed by the Information Commissioner and members of the Management Board and Audit Committee. These individuals must declare any private interests that might affect the carrying out of their duties. They are also required to take steps to resolve any conflicts that arise in a way that protects the

176 Section 105(3B).

177 ICO Code of Conduct (July 2011), available at http://www.ico.gov.uk/about_us/~/media/documents/library/Corporate/Notices/code_of_conduct.ashx (06.03.2012).

178 The Committee on Standards in Public Life is an advisory non-departmental public body established in 1994 and with the original terms of reference to, "examine current concerns about standards of conduct of all holders of public office, including arrangements relating to financial and commercial activities, and to make recommendations as to any changes in present arrangements which might be required to ensure the highest standards of propriety in public life." The Office of the Commissioner for Public Appointments oversees the competitive appointment of seven members, supplemented by three positions nominated by each of the three main political parties. It has no statutory powers and no ability to compel compliance with its recommendations.

179 ICO, Register of Interests, available at http://www.ico.gov.uk/about_us/our_organisation/management_board/~/media/documents/library/Corporate/Practical_application/register_of_interests_policy_and_procedure.ashx (06.03.2013).

	public interest. This Register is made publicly available and is reviewed annually. The ICO also operates a **policy regarding party political activities**[180] which requires staff to obtain permission to take part in national or local party political activities.
Ausgestaltung des Arbeitsverhältnisses	The DPA 1998 specifies that ICO staff, including the Commissioner, are not civil servants.[181] Instead, they are considered as salaried employees of the ICO as an independent non-departmental public body.
Zulässigkeit der **Nebenbeschäftigungen**	There are **no specific regulations** concerning secondary employment, although all staff are subject to the **Code of Conduct** (see above) which constitutes part of their terms and conditions of employment, and requires the disclosure of potential conflicts of interest. Senior staff (the Information Commissioner, members of the Management Board and the Audit Committee) are also expected to complete the **Register of Interests** (see above), which requires declarations on other directorships falling within the Information Commissioner's sphere of statutory responsibility, other relevant employment that might affect the carrying out of duties with the ICO and voluntary and other public offices held.
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	**None**, although all senior management posts are presently listed as full time roles.[182]
Länge der Amtsdauer	The term of office for the Information Commissioner was increased from 5 years to **7 years** by the Protection of Freedoms Act 2012[183] but the possibility for re-appointment under the DPA 1998[184] has now been removed such that a Commissioner may now only serve for a maximum of 7 years. **All other staff appointments are permanent** until normal retirement age unless otherwise indicated. Non-Executive Board Members are appointed for an initial term of three years, renewable by mutual agreement for one further term of a maximum of three years.[185]

180 ICO, Policy and procedure regarding party political activities (December 2008), available at http://www.ico.gov.uk/about_us/~/media/documents/library/Corporate/Notices/political_activities_policy.ashx (06.03.2013).

181 Schedule 5, Part I, section 1(2).

182 See HM Government, Organogram and staff pay data for the Information Commissioner's Office as at 31 March 2012, available at http://data.gov.uk/dataset/staff-organograms-and-pay-ico/resource/9b11a0db-5da7-4092-b8f4-de8e3d13116e (06.03.2012).

183 Section 105(1) Protection of Freedoms Act 2012.

184 Schedule 5, Part I, section 2(5) DPA 1998.

185 Information Commissioner's Annual Report and Financial Statements, Remuneration report, (2011/12) p.53 available at http://www.ico.gov.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/annual_report_2012.ashx (06.03.2012).

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

No literature or other commentary has been found which discusses actual or possible side-line work of the members of senior management; all senior manager posts are full time roles in any event.

3.3. Die Entlöhnung insbesondere

The 2011/12 Remuneration Report of the ICO states that the highest paid director of the Information Commissioner (namely, the Information Commissioner) was £140,000-£145,000, and that this was 5.9 times the median remuneration of the ICO workforce, which was £23,690.

The **Information Commissioner's salary** was increased by 40% from £100,000 per year to £140,000 in November 2008. This followed discussion by Members of Parliament in the House of Commons (the UK's lower house of representatives). The Secretary of State at the time who put forward the motion proposing the increase gave several reasons justifying the level of salary.

First, it was said to acknowledge the increasing importance of the role. Secondly, the workload of the Information Commissioner has increased. Notably, he had had to deal with serial data losses by Government officials, including at Her Majesty's Revenue and Customs, the UK's tax authority. This, accepted some Members of Parliament, had involved him in difficult decisions and in exercising his judgment about what to say publicly on the matter. Thirdly, the increase in salary would not lead to the Information Commissioner being put out of line with other public sector salaries. Members of Parliament from all three main political parties were in broad agreement that the **increase in salary was reasonable and appropriate**.[186]

---

186 See transcript of Hansard on the relevant debate (24 November 2008) available at http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm081124/debtext/81124-0017.htm (06.03.2013).

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	Certain provisions of the DPA 1998 reinforce the independence of the role of the Information Commissioner. These include that he is **constituted as a 'corporation sole'** (see section 2.1 above) and is **not to be regarded as a servant or agent of the Crown** (i.e., the Government);[187] these provisions are supported by the **Framework Agreement**, reiterating the respective duties of the Government Minister and the Information Commissioner (see section 2.2 above) and confirming his or her independence. The Protection of Freedoms Act 2012 has enhanced the independence of future Information Commissioners by requiring that no recommendation may be made to the Queen for the appointment of a person as the Commissioner unless the person concerned has been **selected on merit on the basis of fair and open competition**. The Government has also confirmed that the Minister of Justice's **preferred candidate will be subjected to a pre-appointment hearing** by the cross-party (i.e., involving Members of Parliament from across the political spectrum) House of Commons Justice Committee, who will have the final word on whether or not the candidate should be appointed.[188]
Möglichkeit der **Weisungen von aussen**	The Information Commissioner and his or her office are intended to operate independently, free from the Government and other private interests. The Information Commissioner is nevertheless answerable to Parliament, and it is **Parliament** which in effect retains the authority to remove the Information Commissioner from office, where circumstances justify it.[189] **Certain decisions of the Information Commissioner** were, until the implementation of the Protection of Freedoms Act 2012 however, **subject to approval of the Minister of Justice**. These functions included the need to seek approval on the decisions on the number and terms and conditions of employees,[190] an obligation to consult the Minister before issuing a code of practice or altering a code of practice or associated guidance[191] and a requirement to seek the consent of the Minister for charging fees for ICO services.[192] **Provisions requiring Ministerial approval for these functions have now been removed** from the DPA 1998 and FOIA 2000 by the Protection of Freedoms Act 2012.[193]

187 Schedule 5, Part I, section 1 DPA 1998.

188 See statement of Government Minister, Lord McNally, Hansard, available at http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/110216-wms0001.htm (06.03.2013).

189 Technically, the Queen makes this decision following an Address from both Houses of Parliament. Schedule 5, Part I, section 2(3) DPA 1998.

190 Schedule 5, Paragraph 4 DPA 1998.

191 Sections 41C(7), 52B and 55C(5) DPA 1998.

192 Section 51 DPA 1998; section 47 Freedom of Information Act 2000.

193 Sections 106, 107 and 108.

	In order that the Information Commissioner's independence as a regulator is respected and demonstrated, while still remaining accountable to Parliament for the exercise of his statutory functions and his use of public funds, governmental interference with the office of the Information Commissioner can be said to have been retained for the practical functioning of the office. This is principally in the area of **financial management.** Funding, called 'grant-in-aid', for freedom of information work is determined by the Ministry of Justice in consultation with the Information Commissioner, and the use of any such funding provided must comply with delegated authorities, the Commissioner's own annual budget plans and other conditions imposed by the Ministry. Delegated authorities from the Ministry of Justice to the ICO are subject to public sector expenditure limits, and these are set out in the Framework Agreement (see section 2.2. above)[194], including: • Capital expenditure over £1m; • Acquisition of leasehold interest over £250,000; • Spend on consultancy contracts over £20,000 in value; • Write off of claims for monies owed to the ICO in excess of £50,000; • Special payments, such as compensation and ex gratia payments in excess of £50,000 Other governmental constraints insofar as finance is concerned, relate to **income of the ICO** for its activities, such as fines and other charges which generate profit. Such receipts must be remitted to the Ministry of Justice, as should any income from fees and charges of the ICO not used by the end of the financial year.[195] There also exists an **Information Tribunal**, which, under the DPA 1998 and FOIA 2000, has the power to hear appeals against decisions of the ICO. The ICO must then adhere with the decision of the Information Tribunal, which include the power to quash notices or orders of the ICO and to substitute such other orders or determinations as could have been made by the ICO.[196]
Neutralität der Behörde	The ICO and Information Commissioner personally **do not represent individuals, private parties or political interests**. Their remit is to operate as an independent regulator and supervisory authority with the mission of upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

194 See Appendix A, Framework Agreement, op. cit.

195 See paragraphs 54-57 Framework Agreement, op. cit.

196 Section 49 DPA 1998 and section 58 FOIA 2000.

5. Ressourcen

5.1. Übersicht

Budgethoheit	It has been agreed as part of the Framework Agreement with the Ministry of Justice (see section 2.2. above) that the ICO's corporate and business plans must be supported by three year income and expenditure projections and a detailed annual budget. These projections **do not require governmental or parliamentary approval**. For services and duties carried out under the FOIA 2000, the ICO receives **funding** from the Ministry of Justice, known as **'grant-in-aid'**. The amount of funding is decided following consultation with the Information Commissioner, who will receive a formal statement of the proposed financial provision in advance of each financial year. This financial provision is **subject to parliamentary approval**.
Einnahmequellen der Behörde	Expenditure on data protection activities (i.e., duties of the ICO carried out under the DPA 1998) is financed through the retention of fees collected from data controllers who notify their processing of personal data under the DPA 1998. Data controllers are any individuals, organisations and other corporate or unincorporated bodies which process personal data of individuals ('data subjects') and they must register with the ICO, unless exempt. **Registration and annual renewal requires the payment of a fee**. A fee of £500 applies to organisations with either a turnover of £25.9m and 250 or more employees, or if they are a public authority with 250 or more employees. All other organisations pay £35 per year.[197]
Verfügt die Behörde **über ein eigenes Budget.**	The ICO receives income from a variety of sources. Roughly 65% of its budget funds work on data protection and 35% is work on Freedom of Information. As discussed above, the ICO's data protection responsibilities are funded entirely by fees paid by data controllers, and to this extent, **the ICO does have its own separate budget** in addition to the budget provided for freedom of information work under the 'grant-in-aid'. Being independent from the Government, the Commissioner is responsible for how he deploys the resources granted and received. According to the 2011/2012 Annual Report,[198] fee income is collected and banked into a separate bank account and 'cleared' funds are transferred weekly to the Information Commissioner's administration account to fund expenditure. Fees collected from data controllers in the year 2011/2012 totalled £15,984,000. Such funds as are necessary to meet any liabilities at the end of the financial year (such as creditors) or unspent funds up to a maximum of 3% of total annual notification fee income (whichever is

197 See 'How much does it cost?' on ICO website, available at http://www.ico.gov.uk/for_organisations/data_protection/notification/cost.aspx (11.03.2013).

198 Information Commissioner's Annual Report and Financial Statements, Remuneration report, op. cit. p. 51.

	greater) may be carried over to the following financial year. Funds beyond this must be remitted to the Ministry of Justice. In 2011/2012 for example, £446,000 was forwarded to the Ministry of Justice, representing un-spent data protection fees above the carry forward limits for the year. In addition, civil monetary penalties for serious breaches of the DPA 1998 were levied, amounting to £688,000. These do not form part of the ICO's budget, but are collected and forwarded to the Ministry of Justice.

5.2. Adäquanz des Budgets insbesondere

Around £0.5 million of un-spent data protection fees was forwarded to the Ministry of Justice in both 2010/11 and 2011/12, indicating that data protection fees are more than sufficient for undertaking the data protection work of the ICO.

As to the Government funding for freedom of information work of the ICO (the 'grant-in-aid'), the Constitutional Affairs Select Committee (a grouping of Members of Parliament from across the political spectrum) reported in 2006 that there had been a backlog of complaints concerning freedom of information requests and that, "*we are not convinced that adequate resources have been allocated to resolve the problem, or that they are allocated early enough.*"[199] In its response,[200] the Government stated that the grant in aid for the Commissioner's FOIA work in 2005-6 was £5m, and that the Commissioner had eventually sought additional resources to enable him to clear a backlog of cases that had built up during 2005. Although additional funding was provided, this did not amount the sum he had been seeking; instead, cost savings plus an 11% increase in funding did allow the ICO to eliminate their backlog in 2006-7. The Government stated in its report that it is committed to ensuring that the Information Commissioner is funded adequately to provide a good service to the public.

No further indication is given of the adequacy of the budget in subsequent years. According to the 2011/2012 ICO Annual Report however, it is noted that the grant-in-aid for 2011/12 was only £4.5 million, compared to 2010/11, when it was £7.2 million.

199 House of Commons Constitutional Affairs Committee, Freedom of Information – one year on, Seventh report of Session 2005-06, para. 62 available at http://www.publications.parliament.uk/pa/cm200506/cmselect/cmconst/991/991.pdf (11.03.2013).

200 Government Response to the Constitutional Affairs Select Committee Report, Freedom of Information - one year on (October 2006), available at http://www.official-documents.gov.uk/document/cm69/6937/6937.pdf (11.03.2013).

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	**Section 42 DPA 1998** provides that a request for an assessment (in effect, a 'complaint') as to whether data processing has been carried out in compliance with the provisions of the DPA 1998 **may be made to the Information Commissioner by or on behalf of *any person*** who is or believes themselves to be directly affected by any processing of personal data. Most of the requests for assessment are made by individuals who believe that their data has not been properly processed.
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	When a request for assessment is received by the ICO, an initial view will be formed as to whether the allegation raises the question of whether a criminal offence may have been committed under the DPA 1998 or whether it merely raises an issue of the breach of one or more of the Data Protection principles (see section 1 above). Requests involving potential criminal conduct will be investigated under the provisions of the Police and Criminal Evidence Act 1984 in cooperation with the police. Investigations involving a breach of one or more of the Data Protection principles (i.e., civil conduct) will be subject to an initial assessment as to whether the matter could result in an Enforcement Notice[201] being issued if the allegation was found to be correct. Under section 43 DPA 1998, the Commissioner may serve a document known as an **Information Notice** on any data controller requiring the data controller to furnish certain information to the Commissioner. This is to allow the Commissioner to gather sufficient information to determine whether the data controller is processing data in violation of the DPA 1998. Where the Commissioner is satisfied that a data controller has contravened any of the Data Protection principles, he may serve on the data controller an **Enforcement Notice** requiring the data controller to take specific steps to rectify the contravention or to refrain from processing certain specified personal data. It is a criminal offence to fail to comply with an Enforcement Notice.[202] The Information Commissioner has **powers of entry and inspection[203]** on a data controller's premises where he has obtained a warrant from a judge. The judge must be satisfied that there are reasonable grounds for suspecting that either a data controller has contravened or is contravening any of the Data Protection principles or that an offence has or is being committed.

201 This is one of the options open to the Information Commissioner where an **adverse assessment** is ultimately made. The other options open to him are to take no further action, or to seek a written undertaking from the data controller in respect of the taking of the remedial action.

202 Section 47 DPA 1998.

203 Section 50 DPA 1998.

	The Commissioner has the **power**[204] **to inspect** any personal data recorded in **overseas information systems**. These are the Schengen information system, the Europol information system and the Customs information system - and only for the purpose of assessing whether or not any processing of the data has been or is being carried out in compliance with the DPA 1998. Finally, the ICO has the **power to impose fines** for serious breaches of data protection law, by issuing a Monetary Penalty Notice. The power to fine is a civil, rather than criminal, issue.[205] The maximum fine is presently £500,000. Fines are issued in accordance with ICO-issued guidance.[206]
Weitere Aufgaben der Datenschutzbehörde	A principal duty of ICO is to **educate** people about the legislation concerning data protection. An important part of its role is the issuing of Codes of Practice, guidance, telephone advice and attendance at workshops to ensure as many people as possible are aware of the DPA 1998 and its provisions. From January 2001, the Data Protection Commissioner (now known as the Information Commissioner) took on responsibility for **supervising freedom of information** (see section 1 above). The ICO's main responsibilities are to promote good practice by public authorities in observing the FOIA, to inform the public about the FOIA, to consider complaints about any alleged failure to comply with the FOIA and to issue decision notices and exercise enforcement powers to ensure compliance. Since the entry into force in 2005 of the **Environmental Information Regulations 2004** (SI 2004/3391), the ICO has also been given powers to promote and enforce them. These provide a separate means of access for people who want environmental information. The ICO also has responsibility for overseeing compliance with the **Privacy and Electronic Communications Regulations**[207] which principally concern marketing by telephone and electronic means.

204 Section 54 DPA 1998.

205 According to sections 55A-E DPA 1998, this is in circumstances where there has been a serious contravention of any of the Data Protection principles by the data controller and where such contravention was of a kind likely to cause substantial damage or substantial distress, and either, it was committed deliberately, or the data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.

206 ICO, Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) Data Protection Act 1998 (2012), available at http://www.ico.gov.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.ashx (11.03.2013).

207 As amended in the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208).

6.2. Kompetenzen der Behörde

The principal activity of the Information Commissioner and his staff is acting as regulator for the DPA 1998 and as the supervisory authority for freedom of information and the Environmental and Privacy and Electronic Communications Regulations (see 6.1 above). As mentioned above, roughly 65% of its budget funds work on data protection and 35% is for work on freedom of information.

As already discussed, the **duties of the Information Commissioner** insofar as the Ministry of Justice are concerned, are various, ranging from the provision of annual reports and accounts, making arrangements for audits, and developing corporate and business plans. The ICO's website[208] briefly describes the duties of other key roles, namely those which are those held by members of the Management Board. These are:

- **Director of Operations**: responsible for all the ICO's operational functions, including the following divisions: Customer Contact, Case Resolution, Enforcement and Good Practice. This post also has responsibility for the ICO's offices in the regions.
- **Director of Corporate Services**: responsible for all of the ICO's support functions. The Corporate Services directorate includes the departments responsible for human resources, learning and development, communications and corporate governance, finance, facilities, information governance and IT.
- **Deputy Commissioner with responsibility for the Data Protection supervisory functions of the ICO**: This role has responsibility for oversight of the Strategic Liaison Division which develops and manages the ICO's relations with its key stakeholders. This includes representing the UK on the Article 29 Working Party of European Supervisory Authorities set up under the Data Protection Directive to represent European Member States on such matters.
- **Deputy Commissioner and Director of Freedom of Information for the ICO:** This second Deputy Commissioner has lead responsibility for promoting an enforcing Freedom of Information.

These senior managers are supported by staff across the various offices, and these conduct the various functions required of them to enable the Information Commissioner to discharge his duties. No detailed information is provided, but it is understood that the ICO employs designated data protection and freedom of information caseworkers.

6.3. Akzeptanz und Ansehen

No recent information could be found on the general reputation of the ICO, and this is not something referred to in its own Annual Reports. In November 2009 however, the Department for Business Innovation and Skills commissioned a **review[209] into the work of the ICO** as part of a series of reviews being carried out on the activities of 36 national regulators. This reported that the activities of the ICO were by and large compliant with 'Hampton principles' (standards by which the effectiveness of the regulators were measured), but that there are improvements which can easily be made. Its key findings were that:

- The ICO is taking a **leading role on data protection issues** within the EU, showing strategic leadership on this;

---

208 ICO, Management Board, available at http://www.ico.gov.uk/about_us/our_organisation/management_board.aspx (05.03.2013).

209 Department for Business Innovation and Skills, Information Commissioner's Office, A Hampton Implementation Review Report (November 2009) available at http://www.bis.gov.uk/files/file53510.pdf (11.03.2013).

- The ICO has a **good working relationship with its major stakeholders** but would benefit from developing a more structured approach to stakeholder engagement;
- The ICO **produces extensive, clear and accessible guidance** for businesses and the public;
- The ICO is **generally accessible as an organisation to stakeholders**, with its website and helpline working well. Inevitably, it says, **improvements can be made**, such as increasing resources and training for helpline staff and further improving the structure and search facility of its website.

Other commentary is provided by The Campaign for Freedom of Information, which, also in 2009, published a report[210] complaining that **long delays by the ICO in investigating freedom of information complaints** are undermining the effectiveness of the FOIA.

Analysing nearly 500 formal decision notices issued by the ICO in the 18 months prior to 31 March 2009, it found that on average, it took 19.7 months from the date of a complaint to the ICO to the date on which the ICO's decision on the complaint was issued, and that there was a delay of 2 to 3 years in over a quarter of cases. This, said the report's authors, means that even if the information is ultimately disclosed, it may no longer be of interest or use to the requester, and furthermore that requesters may be so frustrated by the experience that they become reluctant to use the FOIA again.

A report[211] released by the ICO, also in 2009, acknowledged this problem, stating that although more caseworkers and increased productivity had enabled the ICO to close roughly as many cases as it had received for the preceding three years, the continuing increase in the number of free of information complaints and the level of resources available had prevented them from making progress in reducing the backlog of cases.

In the 2011/2012 Annual Report,[212] the ICO states that it achieved its "challenging target" of closing 90% of complaints cases within 6 months of receipt – this being 95% for data protection complaints, and 83% of freedom of information complaints.

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

No literature or other commentary has been uncovered which indicates any conflict between the principal dual roles of the ICO regarding its oversight of freedom of information and data protection. Resources are separately allocated, with freedom of information activities funded by the 'grant-in-aid' from public funds and data protection from the annual registration fees (see section 5.1. above).

Neither activity, therefore, is compromised by the other in terms of financial resources, although it can be seen from the parliamentary debate referred to above (see section 5.2. above) and the criticism by The Campaign for the Freedom of Information (see section 6.3.), that backlogs with freedom of information complaints have historically indicated that increased funding has been needed for enhancing freedom of information functions.

---

210 The Campaign for Freedom of Information, Delays in Investigating Freedom of Information Complaints (July 2009) available at http://www.cfoi.org.uk/pdf/foidelaysreport.pdf (12.03.2013).

211 ICO, The ICO's strategy for the discharge of its Freedom of Information Act and Environmental Information Regulations functions (June 2009) para. 4.3, available at http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/foi_strategy_20090609.pdf (12.03.2013).

212 ICO Annual Report and Financial Statements 2011/2012, op. cit, p.19.

I. Finland

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

Finland has two data protection authorities: the Data Protection Ombudsman and the Data Protection Board.

The office of the Data Protection Ombudsman is an independent authority (in Swedish: chefsämbetsverk) operating in connection with the Ministry of Justice.[213] The Office has about 20 staff, and its budget for 2013, decided by the government, is 1,800,000 EURO. It is run by the Data Protection Ombudsman who is elected by the government for limited but renewable periods of maximum five years. The general principles and instructions for the Office of the Data Protection Ombudsman are regulated by law and government ordinance.[214] The values which provide the basis for its activities and position are justice and independence.[215] The Data Protection Ombudsman's main focus is to guide and control the processing of personal data and to provide related consultation. In particular, the duty of the Data Protection ombudsman is to influence, in advance, compliance with the legislation regarding the keeping of registers by providing general guidance and consultations.

The Data Protection Ombudsman has the right of access to personal data which is being processed, as well as all information needed to verify that personal data is being processed lawfully. The Data Protection Ombudsman is required to issue directions and guidelines, and may order a controller to recognise the right of access of the data subject or to rectify an error and, where necessary, refer the matter to be dealt with by the Data Protection Board. Alternatively, it may report it for prosecution. Moreover, the Data Protection Ombudsman may check if the controllers or their representatives' sector specific codes of conduct for data processing are in conformity with legislation relating to the processing of data. The Ombudsman and the Data Protection Board may under certain circumstances enforce the duty to provide access to data, with recourse to a fine in cases of default.[216] The Data Protection ombudsman may appeal to the Data Protection Board in connection with certain decisions.[217]

The **Data Protection Board** is an independent authority affiliated to the Ministry of Justice. Its budget for 2013, decided by the government, is 15,000 EURO. The seven members of the Board are appointed by the government for a renewable period of three years. Its secretary is appointed by the Ministry of Justice. The general principles and instructions for the Data Protection Board are laid down in legislation and in government ordinances. The Data Protection Board deals with questions of principle relating to the processing of personal data, where these concern the application of the Personal Data Act. It has the right of access to personal data which is being processed, as well as all information needed to verify that personal data is being processed lawfully. The Board also has the

---

213 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/uploads/qz41ii.pdf (15.03.13).

214 Chapter 11 Aricle 119 in the Finnish Constitution (In Swedish Finlands grundlag), The Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389) (in Swedish : Lag om datasekretessnämnden och dataombudsmannen), and Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

215 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/27193.htm (15.03.13).

216 Section 39, 40, 42 and 46 Personal Data Act 523/1999) (in Swedish : personuppgiftslagen).

217 Section 45 Personal Data Act 523/1999).

power to grant permissions and issue orders. It is the most important decision-making agency in personal data matters.[218]

At the request of the Data Protection Ombudsman, the Data Protection Board may: prohibit processing of personal data; compel the person concerned in certain cases to remedy an instance of unlawful conduct or neglect; order under certain circumstances that the operations pertaining to the file be ceased; revoke a permission granted for the processing of personal data.[219]

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Finland has two data protection authorities: the Data Protection Ombudsman (in Swedish: Dataombudsmannen) and the Data Protection Board (In Swedish: Datasekretessnämnden).[220] However, it is the office of the Data Protection Ombudsman that is considered as the main authority. The office of the Data Protection Ombudsman is an independent authority (in Swedish: chefsämbetsverk) operating in connection with the Ministry of Justice.[221] The general principles regarding the office of the Data Protection Ombudsman are regulated by law.[222] The Data Protection Board is an independent authority affiliated to the Ministry of Justice.[223] The Data Protection Board is appointed by the Council of State (the government).[224]
Organisationsform	The Office of the Data Protection Ombudsman is an independent authority (In Swedish: chefsämbetsverk) operating in connection with the Ministry of Justice.[225] The office is run by the Data Protection Ombudsman.[226] The Data Protection Board is a board affiliated to the Ministry of Justice. It consists of a Chair, Deputy Chair and five members. [227]

218 Information from the Ministry of Justice available at http://www.om.fi/en/Etusivu/Ministerio/Neuvottelujalautakunnat/Tietosuojalautakunta (15.03.13).

219 Section 44 Personal Data Act 523/1999).

220 Information from the Ministry of Justice available at http://www.om.fi/en/Etusivu/Ministerio/Neuvottelujalautakunnat/Tietosuojalautakunta (15.03.13).

221 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/uploads/qz41ii.pdf (15.0313).

222 Chapter 11 Aricle 119 in the Finnish Constitution (In Swedish Finlands grundlag) and The Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389) (in Swedish : Lag om datasekretessnämnden och dataombudsmannen).

223 Information from the Ministry of Justice available at http://www.om.fi/en/Etusivu/Ministerio/Neuvottelujalautakunnat/Tietosuojalautakunta (15.03.13).

224 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432) (In Swedish : Förordning om datasekretessnämnden och dataombudsmannen).

225 Chapter 11 Aricle 119 in the Finnish Constitution (In Swedish: Finlands grundlag).

226 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/1560.htm (15.03.13).

227 Information from the Ministry of Justice available at

Grösse	The Office of the Data Protection Ombudsman has about 20 staff. The Data Protection Board consists of a Chair, Deputy Chair, five members and one secretary, hence 8 staff.[228]

2.2. Komplexität und Zusammenwirken der Behörden

The Office of the Data Protection Ombudsman and the Data Protection Board is organized on a national level. There are no regional or local authorities or offices.

The office of the Data Protection Ombudsman is an independent authority (in Swedish: chefsämbetsverk) operating in connection with the Ministry of Justice.[229] The general principles regarding the office of the Data Protection Ombudsman are regulated by law.[230] The Ombudsman guides and controls the processing of personal data and provides related consultations. The Ombudsman exerts power re issues related to the implementation of the right of verification and the correction of personal data. In short, the Ombudsman provides general guidance and consultation, provides guidance towards the compilation of the Codes of Conducts, makes decisions pertaining to compliance with legislation and implementations of the rights of data subjects, must be heard in matters of preparation of legislative or administrative reforms concerning the protection of personal rights and freedoms in the processing of personal data, must be consulted by the public prosecutor prior to bringing charges based on violations of the Personal Data Act, carries out supervision and inspection, participates in international co-operation (Europol, Schengen etc.), and, if measures of guidance and advice have failed to remedy a given situation, the Ombudsman may bring an act of violation to the attention of the Data Protection Board.

The Data Protection Board is an independent authority affiliated to the Ministry of Justice.[231] The Data Protection Board is appointed by the Council of State (the government).[232] The Board processes and makes decisions on issues falling within its scope of action as stated in the Personal Data Act. At the request of the Data Protection Ombudsman, it provides regulations concerning the processing of data. It may also grant controllers[233] permission to process personal data, provided that certain prerequisites are fulfilled. Moreover, it deals with issues that are of principal importance in the implementation of the Personal Data Act, monitors the need to develop legislation concerning the processing of personal data and issues initiatives it deems necessary.[234]

---

http://www.om.fi/en/Etusivu/Ministerio/Neuvottelujalautakunnat/Tietosuojalautakunta (15.03.13) and government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

228 Article 1 and 2 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

229 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/uploads/qz41ii.pdf (15.0313).

230 Chapter 11 Aricle 119 in the Finnish Constitution and The Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

231 Information from the Ministry of Justice available at http://www.om.fi/en/Etusivu/Ministerio/Neuvottelujalautakunnat/Tietosuojalautakunta (15.03.13).

232 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

233 A person, corporation, institution or foundation for whose use a personal data file is set up and who is entitled to determine the use of the file.

234 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/uploads/qz41ii.pdf (15.03.13), see also The Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389) and The Personal Data Act (523/1999).

The **Data Protection Ombudsman** runs the Office of the Data Protection Ombudsman. He or she appoints or employs the staff at the office (except the deputy to the Ombudsman who is Head of Department and appointed by the Ministry of Justice).[235]

Where there are an equal number of votes regarding a matter, the Chair of the **Data Protection Board** has a casting vote.[236]
The Office of the Data Protection Ombudsman and the Data Protection Board have been organized in the same way since they were created in 1987.[237]

Data protection is carried out by two authorities, the Data Protection Ombudsman and the Data Protection Board. As discussed above, their different tasks and competences are laid down in legislation and in a government ordinance. Independently, the Data Protection Ombudsman issues directions and guidelines and, at the request of the Ombudsman, the Data Protection Board provides regulations concerning the processing of data.

The level of dependence / independence of the Data Protection Ombudsman from public authorities such as the Ministry (to which it reports) is a question subject to debate.[238]

There seems to have been no significant debate regarding the disadvantages and advantages of this organisational structure.

---

235 Article 7 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

236 Article 4 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

237 See previous Act on the Data Protection Board and the Data Protection Ombudsman (474/1987).

238 See e.g. J. Numminen, Hur Finland regeras, Helsingfors 1985 p. 146.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	The Data Protection Ombudsman is elected and appointed by the government.[239] The deputy to the Ombudsman who is Head of Department is appointed by the Ministry of Justice.[240] The members of the Data Protection Board are elected and appointed by the government.[241]
Persönliche und fachliche Anforderungen der Behördenmitglieder und Mitarbeitenden	The Data Protection Ombudsman shall have a Master of Law degree, good knowledge of data protection issues and proven leadership skills. The deputy to the Data Protection Ombudsman shall have a Master of Law degree, be familiar with data protection issues and have proven leadership skills. Requirements for all other staff at the Office of the Data Protection Ombudsman Office are University degree or other form of education that the position in question requires.[242] The members of the Data Protection Board shall be familiar with data register activity. The Chair, the Deputy Chair and one member and his deputy shall have a Master of Law degree. Good computer technology skills must also be represented at the Board.[243]
Ausgestaltung des Arbeitsverhältnisses	The Data Protection Ombudsman, with the assistance of his/her deputy (in Swedish: byråchef), runs the Office of the Data Protection Ombudsman.[244] Remaining staff in the Data Protection Ombudsman Office are civil servants.[245] General legislation regarding protection of employment applies to the staff (e.g. proper and substantive reasons for termination of the contract). The members of the Data Protection Board are appointed as board members (in Swedish, Datasekretessnämndens medlemmar).
Zulässigkeit der Nebenbeschäftigungen	The staff at the Office of the Data Protection Ombudsman can pursue a secondary activity/employment provided that, inter alia, it is not pursued during regular working hours and as long as it does not undermine the confidence in his or any other employee's impartiality.[246] No regulations have been found regarding the members of Data Protection Board.

239 Article 7 Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

240 Article 7 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

241 Article 1 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

242 Article 6 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

243 Article 1 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

244 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/1560.htm (15.03.13).

245 Article 6 and 9 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

246 Chapter 4 Article 18 Act on employment of civil servants (19.8.1994/750).

Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	The Data Protection Ombudsman must be free from all other activities and posts he or she pursues when he or she is appointed to the position as Ombudsman.[247] There are no other regulations on full or part time work at the top management level.
Länge der Amtsdauer	The Data Protection Ombudsman is appointed for a limited period, maximum 5 years. The period is renewable and there are no limits as to how many times it can be renewed.[248] The members of the Data Protection Board are appointed for a period of three years. The period is renewable and there are no limits as to how many times it can be renewed.[249]

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

No literature on this matter has been found.

The Data Protection Ombudsman shall be free from all other activities and posts he or she pursues when he or she is appointed to the position as Ombudsman.[250] There are no other regulations on full or part time work at the top management level.

3.3. Die Entlöhnung insbesondere

No information has been found regarding this matter.

247 Article 6 Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

248 Article 6 Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

249 Article 1 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

250 Article 6 Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	The values which form the basis for the activities and the position of the Data Protection Ombudsman are justice and independence.[251] However, there are no explicit provisions laid down in law regarding the independence of the Data Protection Ombudsman nor the members of the Data Protection Board. As discussed above, they are elected and appointed by the government and there is therefore a dependence on the government in this regard. The staff in the Office of the Data Protection Ombudsman are appointed or employed by the Ombudsman.[252]
Möglichkeit der Weisungen von aussen	Instructions for the Data Protection Ombudsman and the Data Protection Board are laid down in legislation and in government ordinances. There are no instructions from other public or private bodies.
Neutralität der Behörde	The Data Protection Ombudsman shall be free from all other activities and positions he or she pursues when he or she is appointed to the position as Ombudsman; as such, the Ombudsman shall not represent any partisan interests.[253] Justice and independence are values which form the basis for the activities and the position of the Ombudsman.[254] There are no regulations regarding the neutrality of the members of the Data Protection Board. As referred to above, the instructions for these two authorities are laid down in legislation and government ordinances. Accordingly, they do not need to consider instructions/requests originating from particular political interests or other stakeholders, but only general instructions from the government.

251 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/27193.htm (15.03.13).

252 Article 7 Government ordinance on the Data Protection Board and the Data Protection Ombudsman (3.6.1994/432).

253 Article 6 Act on the Data Protection Board and the Data Protection Ombudsman (27.5.1994/389).

254 Information from the Office of the Data Protection Ombudsman available at http://www.tietosuoja.fi/27193.htm (15.0313).

5. Ressourcen

5.1. Übersicht

Budgethoheit	The budget for the Office of the Data Protection Ombudsman and for the Data Protection Board is decided each year by the government. There is no Parliamentary scrutiny of the particular budget for these authorities. For 2013, the budget is set at 1,800,000 EURO for the Office of the Data Protection Ombudsman and 15,000 EURO for the Data Protection Board.[255]
Einnahmequellen der Behörde	The Office of the Data Protection Ombudsman can charge a fee for its services.[256]
Verfügt die Behörde über ein eigenes Budget.	Yes, each one of the authorities has their own budget.

5.2. Adäquanz des Budgets insbesondere

An inspection carried out by the deputy Parliamentary Ombudsman 2007 indicated that the resources of the Data Protection Ombudsman are clearly limited.[257] However, since 2007, the budget has increased from 1,300,000 EURO to 1,800,000 EURO 2013.

255 Government proposition for budget 2013 available at http://budjetti.vm.fi/indox/sisalto.jsp?year=2013&lang=sv&maindoc=/2013/tae/hallituksenEsitysRuotsi/hallituksenEsitysRuotsi.xml&id=/2013/tae/hallituksenEsitysRuotsi/YksityiskohtaisetPerustelut/25/01/03/03.html (15.03.13).

256 Justitieministeriets förordning om avgiftsbelagda prestationer som tillhandahålls av Dataombudsmannens byrå (351/2009).

257 Report from the Dataombudsman 2007 available at http://www.tietosuoja.fi/uploads/4a16fld3zz.pdf (15.03.13).

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	If the controller of data (e.g. a company or a public authority) refuses the request of a data subject (the person to whom the personal data pertains) to rectify or erase data in his or her personal data file, the data subject may bring the matter to the attention of the Data Protection Ombudsman.[258] The Office of the Data Protection Ombudsman co-operate with data subjects and controllers and organizations representing them as well as other related bodies, aimed at preventing violation of privacy.[259]
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	The Data Protection Ombudsman and the Data Protection Board have the right of access to personal data which are being processed, as well as all information needed to verify that personal data is being processed lawfully. The Data Protection Ombudsman shall issue directions, guidelines and may order a controller to recognise the right of access of the data subject or to rectify an error and, where necessary, refer the matter to be dealt with by the Data Protection Board, or report it for prosecution. Moreover, the Data Protection Ombudsman may check if the controllers or their representatives' sector specific codes of conduct for data processing are in conformity with legislation relating of the processing of data. The Ombudsman and the Data Protection Board may, under certain circumstances, enforce the duty to provide access to data (with violators subject to a default fine).[260] The Ombudsman may appeal certain decisions from the Data Protection Board.[261] At the request of the Data Protection Ombudsman, the Data Protection Board may: prohibit processing of personal data; compel the person concerned in certain cases to remedy an instance of unlawful conduct or neglect; order, under certain circumstances, that the operations pertaining to the file be ceased; revoke a permission granted for the processing of personal data.[262]
Weitere Aufgaben der Datenschutzbehörde	The Data Protection Ombudsman and the Data Protection Board are only responsible / concerned with data protection.

258 Section 29(2) Personal Data Act (523/1999).

259 Information from the Office of the Data Protection Ombudsman p. 3, available at http://www.tietosuoja.fi/uploads/qz41ii.pdf (15.03.13).

260 Section 39, 40, 42 and 46 Personal Data (Act 523/1999).

261 Section 45 Personal Data Act (523/1999).

262 Section 44 Personal Data Act (523/1999).

6.2. Kompetenzen der Behörde

The Data Protection Ombudsman's main focus is to guide and control the processing of personal data and to provide related consultation. The primary duty of the Data Protection ombudsman is to influence, in advance, compliance with the legislation regarding the keeping of registers by providing general guidance and consultations. The Data Protection Board deals with issues that are of principal importance in the implementation of the Personal Data Act, monitors the need to develop legislation and issues initiatives it deems necessary. Since focus is on providing general guidance and consultations, more resources are allocated to the Office of the Data Protection Ombudsman than to the Data Protection Board.

6.3. Akzeptanz und Ansehen

No literature has been found in this regard.

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

The Data Protection Ombudsman and the Data protection Board are authorities responsible for / concerned with data protection, and not the freedom of information. There are therefore no double roles.

J. Slowenien

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

The National Assembly of the Republic of Slovenia adopted the **Information Commissioner Act**[263] (hereinafter: the ICA), on the basis of which an **autonomous and independent state authority** was established on 31 December 2005. The aforementioned Act merged two authorities, the Commissioner for Access to Public Information, which prior to that had the status of an independent authority, and the **Inspectorate for Personal Data Protection**, which had operated as a constituent authority within the Ministry of Justice. Upon the implementation of the ICA, the **Commissioner for Access to Public Information** continued its work as the Information Commissioner, whereby the inspectors and other employees of the Inspectorate for Personal Data Protection and its equipment and resources came under its competence. Concurrently, it also assumed responsibility for all cases, archives, and records of the Inspectorate for Personal Data Protection. Thus, the jurisdiction of the authority that had previously been responsible for ensuring unimpeded access to public information transformed and expanded to encompass personal data protection. As such, the Information Commissioner became a **national supervisory authority for personal data protection** and commenced operations on 1 January 2006.

With such regulation, the practices of the two authorities became uniform, and the right to privacy and the right to know are,as a result of **this regulation, ever more harmonised**. The Head of the Information Commissioner, who has the position of a state official, is appointed by the National Assembly of the Republic of Slovenia.

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the recommendation of the Information Commissioner (Article 5 of the Information Commissioner Act).

In accordance with Article 2 of the ICA, the Information Commissioner is - in the area of data protection - competent to:

- **organize and manage** the work of all employees, including **the national supervisors for personal data protection**;
- **decide on appeals against a decision by which an authority denies or refuses the applicant's request** for access or in any other manner violated the right to access or re-use public information, and also, within the frame of appellate proceedings, to supervise the implementation of the Act regulating access to public information and regulations adopted thereunder (as the appellate authority in the area of access to public information);
- **perform inspections** regarding the implementation of the Act and other regulations **governing the protection or processing of personal data** or the transfer of personal data out of the Republic of Slovenia, as well as to perform other duties determined by these regulations;
- **decide on the appeal of an individual against the refusal of a data controller** to grant the request of the individual with regard to his right to access requested data, and to extracts, lists, viewings, certificates, information, explanations, transcripts, or copies in accordance with the provisions of the act governing personal data protection;
- **file a request before the Constitutional Court of the Republic of Slovenia** for the review of the constitutionality of a law, regulation, or general act issued for the exercise of public

263 Zakon o Informacijskem pooblaščencu, Official Gazette RS, No. 113/2005 – 51/2007–ZUstS-A

authority if a question of constitutionality or legality arises in connection with proceedings it is conducting, in both the field of access to public information and personal data protection.

The Information Commissioner is also the authority **competent to determine and punish offences** and to carry out supervision with regard to the implementation of the Information Commissioner Act, the Access to Public Information Act with regard to the appeals procedure, Article 45 of the Public Media Act, and the Personal Data Protection Act[264] (hereinafter: PDPA).

The Personal Data Protection Act was adopted by the National Assembly of the Republic of Slovenia on 15 July 2004, and has been in force since 1 January 2005. The adoption of this Act was primarily necessary due to the accession of the Republic of Slovenia to the European Union, and the resulting obligation to harmonise personal data protection with the provisions of Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[265]

In accordance with the provision of Article 48 of the PDPA, the **Information Commissioner issues prior opinions to ministries, the National Assembly, self-governing local community bodies, other state bodies, and bearers of public authority** regarding the compliance of the provisions of draft laws and other regulations with the acts and other regulations regulating personal data. In 2011, the Information Commissioner participated in the preparation of more than 30 laws and other regulations.[266]

---

264 Zakon o varstvu osebnih podatkov, Official Gazette RS, No. 86/2004, Official Gazette RS, No. 94/2007 - official consolidated text.

265 Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, No. L 281, 23 November 1995.

266 Letno poročilo Informacijskega pooblaščenca za leto 2011, p. 4, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf <11.04.2013>;

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	According to the **Information Commissioner Act,** the Information Commissioner is an autonomous and independent state authority (ICA Art. 2).
Organisationsform	The Information Commissioner works autonomously with the support of his office. The internal organisation of the Information Commissioner and the structure of professional positions is set by the Information Commissioner in the Act on the Internal Organisation and Post Classification of the Information Commissioner.
Grösse	At the end of 2011, the Information Commissioner had 33 employees.

2.2. Komplexität und Zusammenwirken der Behörden

The **Information Commissioner** is organized and pursues its work on a national level. There are no regional or local authorities or offices.

The **Information Commissioner** is an independent, monocratic, one-person authority. The **Information Commissioner Act** and the regulation of activities of the **Information Commissioner** were adopted by Slovenian Parliament as the best possible **regulation**. No considerable concurring propositions (to our knowledge) were presented. No literature or other commentary has been found which discusses this topic.

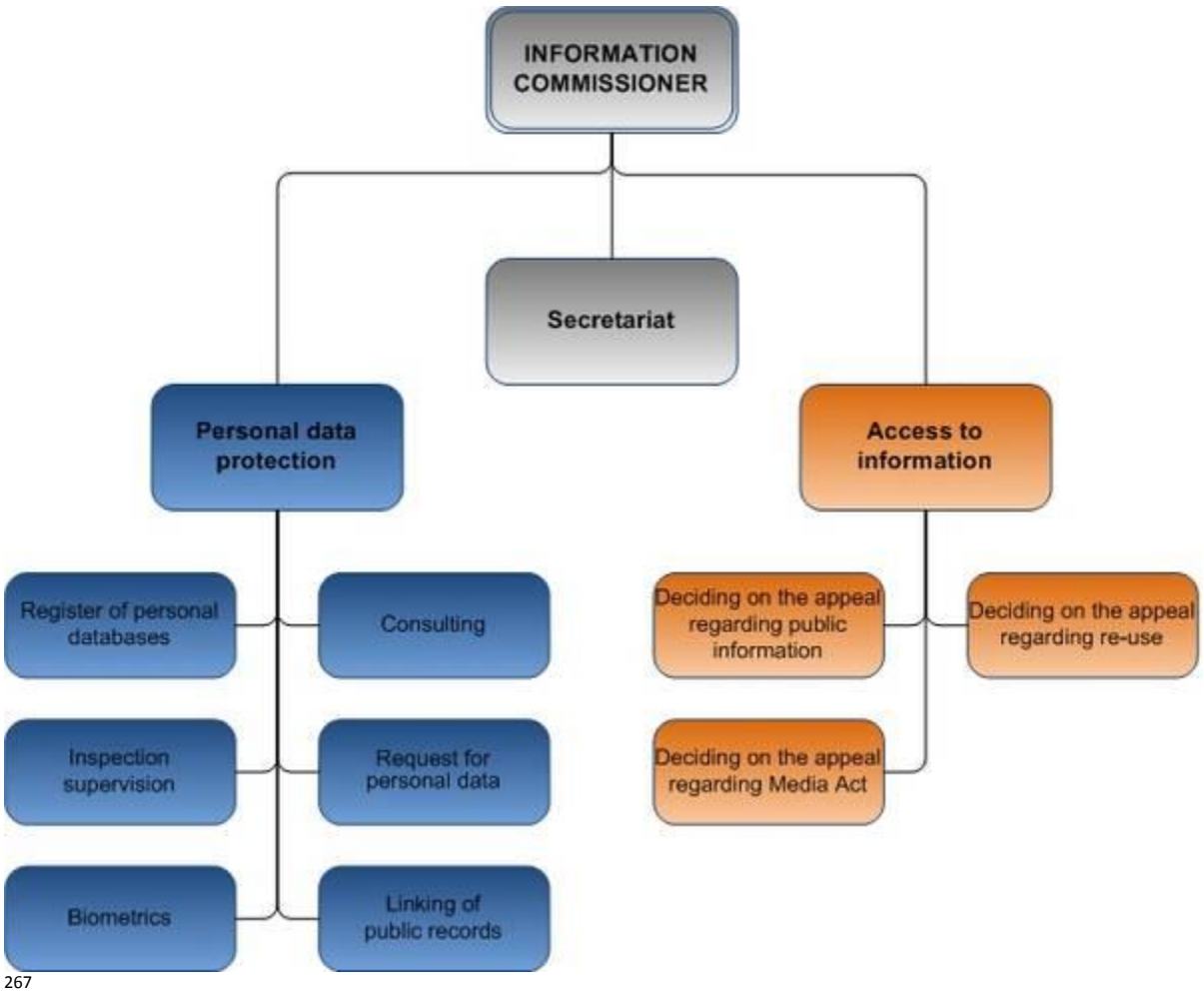
The **Information Commissioner** is solely subject to the provisions governed by the **Information Commissioner Act.** According to the legal regulation, the Slovenian **Information Commissioner** is considered as independent, impartial and neutral (Art. 2 ICA) and the general principles regarding the office of the **Information Commissioner** are regulated by law.

The **Information Commissioner Act** merged two authorities, the Commissioner for Access to Public Information, which prior to that had the status of an independent authority, and the **Inspectorate for Personal Data Protection**, which had operated as a constituent authority within the Ministry of Justice. Upon the implementation of the ICA, the **Commissioner for Access to Public Information** continued its work as the Information Commissioner, whereby the inspectors and other employees of the Inspectorate for Personal Data Protection and its equipment and resources came under its competence.

The internal organisation of the Information Commissioner and the structure of professional positions therein required to carry out its tasks are determined by the Act on the Internal Organisation and Post Classification of the Information Commissioner and the annex thereto, i.e. the Classification of Posts within the Information Commissioner. The classification of positions is adapted to the tasks and duties of the Information Commissioner and the work processes carried out therein, and is designed such that it ensures the most effective use of human resources.

The Information Commissioner carries out its tasks through the following organisational units:
- The Secretariat of the Information Commissioner
- The Public Information Department
- The Personal Data Protection Department
- Administrative and Technical Services.

Organisation of the Information Commissioner:



267

The Personal Data Protection Act was adopted by the National Assembly of the Republic of Slovenia on 15 July 2004, and has been in force since 1 January 2005. The adoption of this Act and the **Information Commissioner Act** was primarily necessary due to the accession of the Republic of Slovenia to the European Union, and the resulting obligation to harmonise personal data protection

267 https://www.ip-rs.si/o-pooblascencu/zaposleni/ <11.04.2013>

with the provisions of Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[268] There seems to have been no significant debate regarding the disadvantages and advantages of this type of organizational scheme.

Competencies of the Information Commissioner under the Personal Data Protection Act, are:

1. performing supervision of the implementation of the provisions of the Personal data protection Act (PDPA), (handle cases of complaints, appeals, notifications and other applications, explaining possible breach of law);
2. issuing supervision measures based on Art. 54 of PDPA (prohibition to process personal data, applying anonymity, blocking, erasing or destroying personal data, when established that the data is not processed according to the law;
3. issuing other supervision measures in accordance with the Act governing inspection supervisions and the Act governing general administrative procedures (Point 5, Para. 1 Art. 54 of PDPA);
4. performing preventive supervision with personal data controllers in public and private sectors;
5. managing and maintaining a register of personal databases, ensuring its updating and public internet access (Art. 28 of PDPA);
6. ensuring the viewing and transcription of data from the database register (as a rule on the same day or in eight days at the latest – Art. 29 of PDPA);
7. performing procedures with regard to violations in the field of personal data protection (expedient procedure);
8. filing a criminal information or perform procedures in accordance with the Act governing violations, if during an inspection, a suspicion of criminal offence or violation arises;
9. deciding on an individual's complaint with regard to processing of personal data based on Art. 9(4) and Art. 10(3) of PDPA;
10. issuing decisions on ensuring an adequate level of personal data protection in third countries (Art. 63 of PDPA);
11. performing procedures to assess an adequate level of personal data protection in third countries based on findings of supervisions and other information (Art. 64 of PDPA);
12. managing a list of third countries ascertained to have partially or entirely adequate or inadequate personal data protection levels; in case only a partial adequacy of personal data protection is ascertained, the list will also state the scope of adequate protection (Art. 66 of PDPA).
13. managing administrative procedures to issue permissions to transfer personal data to a third country (Art. 70 of PDPA);
14. managing administrative procedures to issue permissions to link public records and registers, in cases when at least one of the personal databases to be linked contains sensitive personal data or if implementation of the linking requires the use of the same connecting code (such as the standardized personal registration number or tax number);
15. managing administrative procedures to issue declaring decisions on whether a planned implementation of biometric measures in private sector accords with the provisions of PDPA;
16. working with government bodies, competent EU bodies for protection of individuals with regard to processing personal data, international organizations, foreign personal data protection bodies, institutions, associations, and other bodies and organizations with regard to questions of personal data protection;

---

268 Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, No. L 281, 23 November 1995.

17. issuing and publishing preliminary opinions to state bodies and public powers holders on harmonizing the provisions of proposals of legislation with Acts and other legislation governing personal data;
18. issuing and publishing non-obligatory opinions on the conformity of professional ethics codes, general conditions of business or the proposals thereof, with regulations in the field of personal data protection;
19. preparing, issuing and publishing non-obligatory recommendations and instructions with regard to personal data protection in a particular field;
20. the publication on internet pages or in other appropriate ways of preliminary opinions on compliance with positive Acts and other legislation of proposals of Acts and other regulations in the field of personal data protection as well as publication of requests for constitutional review of statutes (Art. 48 of PDPA), issuing internal bulletin and expert publications, publishing decisions and court resolutions dealing with personal data protection, as well as non-obligatory opinions, explanations, positions and recommendations with regard to personal data protection (Art. 49 of PDPA);
21. issuing press releases on performed supervisions and preparing annual reports on its work in the current year;
22. Information Commissioner is an appellate body, competent for supervising the implementation of the Information Commissioner Act, the Act on access to public information within the frame of its appellate proceedings and the Act on personal data protection;
23. deciding on the appeal of an individual when the data controller refuses his request for access to data relating to him, or, requesting for extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the Act governing personal data protection (competency established in the Information Commissioner Act);
24. Information Commissioner also participates in working groups for personal data protection, formed within the EU framework and bringing together independent bodies for protection of personal data in member states.

In accordance with the provision of Article 48 of the PDPA, the **Information Commissioner issues prior opinions to ministries, the National Assembly, self-governing local community bodies, other state bodies, and bearers of public authority** regarding the compliance of the provisions of draft laws and other regulations with the Acts and other regulations regulating personal data. In 2011, the Information Commissioner participated in the preparation of more than 30 laws and other regulations (in 2010 more than 50).[269]

[269] Letno poročilo Informacijskega pooblaščenca za leto 2011, p. 63, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf, <11.04.2013>; Letno poročilo Informacijskega pooblaščenca za leto 2010, p. 59-60, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf, <11.04.2013>

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	Information Commissioner is appointed by the National Assembly of the Republic of Slovenia on proposal of the president of the Republic of Slovenia (ICA Art. 6/1).
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	For the appointment as Information Commissioner, a person must fulfil the following conditions: - be a citizen of the Republic of Slovenia; - hold a university degree; - have at least five years of working experience; - must not have been convicted by a final decision of a criminal offence punishable by an unconditional punishment of deprivation of liberty (ICA Art.6/2).
Ausgestaltung des Arbeitsverhältnisses	Information Commissioner has the status of Officer of State. Information Commissioner may be subject to early dismissal by the National Assembly of the Republic of Slovenia only if: - he himself so demands, - if he no longer fulfils the conditions for execution of the function determined in the ICA. - if he becomes permanently incapable of performing his function, - if he neglects to execute his powers in accordance with the Law and Constitution. The procedure for the dismissal of the Information Commissioner shall be initiated on the recommendation of the president of the Republic of Slovenia (ICA Art.7).
Zulässigkeit der **Nebenbeschäftigungen**	The holding of the office of the **Information Commissioner** is incompatible with the holding of any office in the state bodies, local self-government bodies, political parties and trade unions, or the performing of other functions and activities which are incompatible by law with the holding of a public office. If the **Information Commissioner** does not discontinue a profitable activity incompatible by law with the performing of the function of the **Information Commissioner** within 30 days of the day when the competent committee at the Parliament has declared such incompatibility, his office as **Information Commissioner** shall be terminated (ICA Art.7/4). Remaining staff of the **Information Commissioner** Office are civil servants. General legislation regarding protection of employment applies to the staff (e.g. proper and susbstantive reasons for termination of the contract).
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	Position of the **Information Commissioner** is considered as a full time job.
Länge der Amtsdauer	**Information Commissioner** is appointed for a five year term and can be reappointed once (ICA Art. 6/3).

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

Position of the **Information Commissioner** is considered as full time job. Research has not revealed any further information on this topic. No literature or other commentary which discusses actual or possible side-line work of the employees of the **Information Commissioner office** has been found; according to the annual report of the Institution, all employees' posts are rated as full time roles. At the end of 2011, the Information Commissioner had 33 employees, of which five were employed on the basis of temporary contracts. Three of the temporary employees were substituting for employees on leave, while two were trainees. All employees in official positions have at least a bachelor's degree.[270]

3.3. Die Entlöhnung insbesondere

No information.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	With regard to the performance of the duties entrusted to the **Information Commissioner**, he/she is solely subject to the provisions governed by the ICA (Art.2 ICA).
Möglichkeit der **Weisungen von aussen**	No legal possibility for instructions from outside.
Neutralität der Behörde	The **Information Commissioner** may not be a member of any political party or be involved in any public activity which is not consistent with the integrity of the **Information Commissioner's** post. The Institution is considered as neutral (impartial and independent).

5. Ressourcen

5.1. Übersicht

Budgethoheit	Self-standing accounting item in the Law on State budget adopted by the Parliament
Einnahmequellen der Behörde	The State budget. The Institution applies no charges.
Verfügt die Behörde **über ein eigenes Budget.**	Yes. Independent budget set by the Parliament.

[270] Letno poročilo Informacijskega pooblaščenca za leto 2011, p. 5. https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf; <11.04.2013>

5.2. Adäquanz des Budgets insbesondere

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the recommendation of the Information Commissioner (Article 5 of the Information Commissioner Act). In the fiscal year 2010, the funding allocated to the Information Commissioner at the start of the year amounted to EUR 1,421,664.68. Of this, EUR 895.45 was brought forward from the previous year's allocation, under Budgetary Items 7459 and 7460, as well as EUR 5,974.53 of European funding from the European Privacy Open Space project, under Item 9378. During the year the Information Commissioner received EUR 11,400.00 of European funding for participation in the LAPSI project, under Item 9586. Of these funds, EUR 6,628.34 were used in 2010, while the remaining funds were brought forward to 2011.

At the end of 2010, the Information Commissioner received EUR 67,407.60 of European funding for participation in the Twinning project, of which EUR 2,524.80 was used in 2010, with the remainder brought forward to 2011. In order to increase savings in the state budget, the Information Commissioner returned EUR 13,000.00 to the budget from Item 1267 (wages and salaries). The Information Commissioner reassigned EUR 2,113.51 from Item 1271 (material costs and expenses) to Item 1273 (investments), and 1,500.00 EUR to Item 1267 (wages and salaries).

In 2010, the Information Commissioner used EUR 1,386,158.63 of budgetary funding, of which:

- EUR 1,038,430.43 were for wages and salaries and other employee expenses;
- EUR 325,614.69 were for material costs and expenses;
- EUR 22,113.51 were for investments and capital expenditure.

The operational budget at year end amounted to EUR 1,502,972.58. European funds for the implementation of the LAPSI and Twinning projects are included in this amount. Excluding earmarked and European funds, 98.88% of the budget was used, while the figure is 94.27% taking into account revenues due to European funding.[271]

---

271 Letno poročilo Informacijskega pooblaščenca za leto 2010, p. 5, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2010_net.pdf, <11.04.2013>

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	Individuals can make a request / file a complaint with Information Commissioner. Such request can lead to an inspection. An individual who finds that his rights provided by PDPA have been violated may request judicial protection for as long as such violation lasts (Article 34 PDPA).
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	In order to perform his/her tasks, the Information Commissioner may address state authorities, territorial self-government authorities, as well as state and municipal organizational units, private entities performing public tasks, natural and legal persons, organizational units without legal personality and other entities in order to ensure efficient protection of personal data. In order to fulfil its supervisory function, the Information Commissioner is entitled to obtain on request: access to personal data that is processed; information and documentation about the processing of personal data and security of this processing; and access to those premises linked to the processing of personal data. The Information Commissioner may also request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relative to personal data protection. The Supervisor (delegated by the Information Commissioner) who, in performing inspection supervision, detects a violation of PDPA or of another statute or regulation regulating protection of personal data has the right immediately: 1. to order the elimination of irregularities or deficiencies he detects in the manner and within the interval he himself defines; 2. to order the prohibition of processing of personal data by persons in the public or private sector who have failed to ensure or failed to implement measures and procedures to secure personal data; 3. to order the prohibition of processing of personal data and the anonymising, blocking, erasure or destruction of personal data whenever he concludes that the personal data is being processed in contravention of the statutory provisions; 4. to order the prohibition of the transfer of personal data to third countries, or their supply to foreign data recipients if they are transferred or supplied in contravention of statutory provisions or binding international treaties; 5. to order other measures provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure (Article 54 PDPA).
Weitere Aufgaben der Datenschutzbehörde	The Information Commissioner has twofold status: first, as the authority for Access to Public Information and, secondly, as authority for Personal Data Protection.

6.2. Kompetenzen der Behörde

Competencies of the Information Commissioner under the Personal Data Protection Act, are e.g.:

- supervising the implementation of the provisions of PDPA (handle cases of complaints, appeals, notifications and other applications, explaining possible breaches of law);
- issuing supervision measures based on Art. 54 of PDPA (prohibition to process personal data, anonymising, blocking, erasing or destroying personal data, when established that the data is not processed according to the law;
- issuing other supervision measures in accordance with the Act governing inspection supervisions and the Act governing general administrative procedure (Point 5, Para. 1 Art. 54 of PDPA);
- performing preventive supervision with personal data controllers in public and private sectors;
- managing and maintain a register of personal databases, ensure its updating and public internet access (Art. 28 of PDPA);

The Information Commissioner is also an appellate body, competent for supervising the implementation of the Information Commissioner Act, the Act on access to public information within the frame of its appellate proceedings and the Act on personal data protection. This extends to deciding on the appeal of an individual when the data controller refuses his request for access to data relating to him or on requests for extraction, listing, examination, confirmation, information, explanation, transcript or copies in accordance with provisions of the Act governing personal data protection (competency established in ICA).

Within the framework of inspection supervision, the Information Commissioner supervises:

- the lawfulness of processing of personal data;
- the suitability of measures for security of personal data and the implementation of procedures and measures for security of personal data pursuant to PDPA;
- the implementation of the provisions of the statute regulating the filing system catalogue, the Register of Filing Systems and the recording of the supply of personal data to individual data recipients;
- the implementation of the statutory provisions regarding the transfer of personal data to third countries and on the supply thereof to foreign data recipients (Article 51 PDPA).

In performing inspection supervision, the Information Commissioner is entitled:

1. to examine documentation relating to the processing of personal data, irrespective of their confidentiality or secrecy, and the transfer of personal data to third countries and the supply to foreign data recipients;
2. to examine the contents of filing systems, irrespective of their confidentiality or secrecy, and filing system catalogues;
3. to examine documentation and acts regulating the security of personal data;
4. to examine premises in which personal data is processed, computer and other equipment, and technical documentation;
5. to verify measures and procedures to secure personal data, and the implementation thereof;
6. to exercise other competences provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure (Article 53 PDPA).

In the area of access to public information, the Information Commissioner has the competences determined by Article 45 of the Public Media Act[272] (hereinafter: the PMA). In accordance with the

[272] Zakon o medijih, Official Gazette RS, No. 110/2006, official consolidated text.

PMA, a liable authority's refusal of a request by a representative of the media will be deemed a decision refusing the request. The lack of a response of an authority following such a request is a violation and provides grounds for an appeal. The Information Commissioner decides on an appeal against a decision refusing a request in accordance with the provisions of the Access to Public Information Act[273] (hereinafter: APIA).

The Information Commissioner also has the following competences under the Electronic Communications Act[274]5 (hereinafter: the ECA):

- to carry out inspections of retained traffic and location data acquired or processed in connection with providing public communication networks or services in accordance with Articles 107.a to 107.e of the ECA (the second paragraph of Article 112 of the ECA);
- in the area it supervises, to adjudicate on offences which amount to a violation of the ECA and regulations issued on the basis thereof, the Information Commissioner being the authority competent to determine and punish offences in accordance with the Act regulating offences (Article 147 of the ECA);
- to prevent abuses and proper implementation of the European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and the amended Directive on the retention of telecommunications data.

The Information Commissioner also assumes responsibility for supervision of the implementation of Article 128 of the Schengen Convention (the Convention implementing the Schengen Agreement) and is thus an independent body responsible for supervising the transfer of personal data for the purposes of the mentioned Convention.

In 2008, the Information Commissioner acquired competences pursuant to the Patients' Rights Act[275], the Identity Card Act[276], and the Travel Documents Act[277].

Under the Patients' Rights Act (hereinafter: the PRA), the Information Commissioner has the following competences:

- to decide on appeals by patients and other entitled persons in cases of a violation of the provision regulating the manner of access to medical records; in this procedure the provider of health care services is regarded as the first instance authority (the tenth paragraph of Article 41 of the PRA);
- to decide on appeals by persons defined by the Act against partial or total refusal of any request for access to medical records following the death of a patient (the fifth paragraph of Article 45 of the PRA);
- to decide on appeals by entitled persons against partial or total refusal of any request for access which refers to the duty to protect information on the medical condition of a patient, provided that it concerns information which originates from medical records (the seventh paragraph of Article 45 of the PRA).

On the basis of the Identity Card Act (hereinafter: ICA), the Information Commissioner has the following competences:

---

273 Zakon o dostopu do informacij javnega značaja, Official Gazette RS, Nos. 51/2006 and 117/2006.

274 Zakon o elektronskih komunikacijah, Official Gazette RS, No. 13/2007 official consolidated text.

275 Zakon o pacientovih pravicah, Official Gazette RS, No. 15/2008.

276 Zakon o osebni izkaznici, Official Gazette RS, No. 71/2008 – official consolidated text.

277 Zakon o potnih listinah, Official Gazette RS, No. 62/2009 – official consolidated text.

- to carry out supervision of the implementation of Article 3a of the ICA, which regulates the instances and manner in which the data controller is permitted to copy personal identity cards, and determines the manner in which copies may be stored;
- in the event of a violation of the provision of Article 3a of the ICA, to determine and punish the offence as the competent authority, in accordance with Article 19a of the ICA.

On the basis of the Travel Documents Act (hereinafter: TDA), the Information Commissioner has the following competences:

- to carry out supervision of the implementation of Article 4a of the TDA, which regulates the instances and manner in which the data controller is permitted to copy passports, and determines the manner in which copies may be stored;
- in the event of a violation of the mentioned Article 4a of the TDA, to determine and punish the offence as the competent authority, in accordance with Article 34a of the TDA.

In 2009, the Information Commissioner also gained the following competences under the Banking Act[278] (hereinafter: BA):

- to give its consent to the administrators of the SISBON system prior to the application of the system's rules referred to in point 1 of paragraph 13 of Article 309a of the BA, which determines that the administrator must adopt the rules of the system, wherein he determines the technical conditions for members, i.e. banks, to access the system and other measures for the security of personal data (paragraph 14 of Article 390a of the BA);
- to carry out supervision of the implementation of Article 309a of the BA, which regulates the collection, processing, and system of exchange of information on the credit rating of clients and, in accordance with Article 397 of the BA, to conduct procedures deciding on offences.

6.3. Akzeptanz und Ansehen

According to research carried out by the Public Opinion and Mass Communication Research Centre, as of February 2010, the level of trust in the Information Commissioner was characteristically high (53.1%), while the level of distrust was the lowest of all the institutions monitored (12.2%)[279].

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

ICA merged two authorities, the **Commissioner for Access to Public Information**, which prior to that had the status of an independent authority, and the **Inspectorate for Personal Data Protection**, which had operated as a constituent authority within the Ministry of Justice. Thus, the jurisdiction of the authority that had previously been responsible for ensuring unimpeded access to public information transformed, and expanded to encompass personal data protection. As such, the Information Commissioner became a **national supervisory authority for personal data protection.** According to the Slovenian commentary with such regulation the practices of the two authorities became uniform; at the same time, the right to privacy and the right to know are, as a result of **this regulation, ever more harmonised**.[280] "Personal data protection has not been instituted as a concretisation of the right for privacy in the field of personal data processing only; it also serves for

---

278 Zakon o bančništvu, Official Gazette RS, No. 131/2006, with amendments.

279 Letno poročilo Informacijskega pooblaščenca za leto 2010, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2010_net.pdf, <11.04.2013>

280 Letno poročilo Informacijskega pooblaščenca za leto 2011, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf, <11.04.2013>

the protection of information privacy."[281] **No literature or other commentary** has been uncovered which indicates any conflict between the principal dual roles of the Information Commissioner of overseeing both freedom of information and data protection.

281 N. Pirc Musar, Personal data protection in view of the freedom of expression and protection of privacy, https://www.iprs.si/fileadmin/user_upload/Pdf/clanki/Personal_data_protection_in_view_of_the_freedom_of_expression_and_protection_of_privacy.pdf <11.04.2013>

K. Spanien

1. Zusammenfassende Beschreibung der Organisationsform und Zuständigkeiten der Datenschutzbehörde

En vertu de la Loi organique 15/99 (LO 15/99) , l'Agence espagnole de protection des données (AEPD) est chargée de veiller à l'application de la législation sur la protection des données dans ce pays. L'AEPD est une institution de droit public, dotée d'une personnalité juridique propre et de la capacité pour agir indépendamment des pouvoirs publics et de l'administration, dans les domaines public et privé. L'AEPD élabore et approuve chaque année l'avant-projet de son budget annuel et l'adresse au gouvernement pour qu'il soit incorporé au budget général de l'État en tant qu'élément indépendant.

Du point de vue organisationnel, au sommet de la pyramide hiérarchique de l'AEPD se trouvent le Directeur et le Conseil consultatif (*Consejo consultivo*), en dessous desquels on compte un Registre général de protection de données, une Inspection de données, un Secrétariat général et une unité de Relations internationales.

Mis à part l'AEPD, il existe d'autres entités compétentes dans le domaine de la protection de données, notamment au niveau de certaines régions, comme la Catalogne, le Pays Basque et Madrid. Ces autorités – qui jouissent d'indépendance pour accomplir leurs tâches - doivent toutefois agir dans la stricte sphère des compétences attribuées aux régions par la Constitution espagnole et en articulation avec les compétences de l'AEPD. Ceci dit, les entités régionales ne peuvent pas empiéter sur les compétences que l'AEPD possède au niveau national .

Les tâches de l'AEPD ont un caractère principalement préventif, ce qui correspond au modèle adopté par les États voisins de l'Espagne . En outre, l'AEPD a aussi le pouvoir d'imposer des sanctions et de prendre des mesures préventives en cas de violations des dispositions de la loi espagnole sur la protection de données. Afin d'accomplir ses tâches, l'AEPD a été investie de pouvoirs d'enquête ou d'inspection (potestad de investigación o de inspección).

Les compétences de l'AEPD sont, entre autres, les suivantes :

a) veiller au respect de la législation relative à la protection des données et contrôler son application, en particulier en ce qui concerne les droits d'information, d'accès, de rectification, d'opposition et d'annulation des données;
b) délivrer les autorisations prévues par la législation relative à la protection des données;
c) émettre, le cas échéant, et sans préjudice des compétences d'autres organes, les instructions nécessaires pour rendre les traitements conformes aux principes de la législation relative à la protection des données;
d) répondre aux demandes et réclamations formulées par les personnes concernées;
e) informer les personnes sur leurs droits en matière de traitement des données à caractère personnel;
f) requérir des responsables et des personnes chargées des traitements, après audience de ces derniers, qu'ils prennent les mesures nécessaires à la mise en conformité du traitement des données aux dispositions de la législation relative à la protection des données et, le cas échéant, ordonner la cessation des traitements et l'annulation des fichiers, en cas de non-conformité aux dispositions légales;
g) exercer le pouvoir de sanction dans les termes prévus au titre VII de la législation relative à la protection des données;
h) établir les rapports à caractère obligatoire sur les projets de dispositions générales d'application de la législation relative à la protection des données;

i) recueillir auprès des responsables des fichiers toute aide et information jugées nécessaires à l'exercice de ses fonctions;
j) assurer la publicité de l'existence de fichiers des données à caractère personnel, et, à cet effet, publier périodiquement une liste desdits fichiers contenant l'information supplémentaire requise par le Directeur de l'Agence;
k) rédiger un mémoire annuel et l'adresser au Ministère de la Justice;
l) exercer le contrôle et accorder les autorisations pertinentes en rapport avec les flux internationaux de données ainsi qu'exercer les fonctions de coopération internationale en matière de protection des données à caractère personnel;
m) veiller à l'accomplissement des dispositions que la loi sur la fonction publique établit concernant la collecte de données statistiques et le secret statistique, ainsi que dicter les instructions nécessaires, exprimer un avis sur les conditions de sécurité des fichiers constitués à des fins exclusivement statistiques et exercer le pouvoir de sanction pour les violations commises au sein des administrations publiques;
n) toute autre compétence attribuée par la loi.

Compte tenu de ces pouvoirs étendus ainsi que de la large indépendance attribuée à l'AEPD, il faut conclure, en cas de doute, en faveur des attributions de l'AEPD .

2. Allgemeine Ausgestaltung der Behörde

2.1. Übersicht

Stellung der Behörde	Selon la LO 15/99, l'AEPD est une **entité indépendante de droit public**.
Organisationsform	L'AEPD est une agence qui agit de façon indépendante. Le Directeur jouit de larges pouvoirs au sommet de la pyramide. L'organisation interne et la structure de l'AEPD est réglée par la LO 15/99 et par un Statut adopté par le gouvernement.
Grösse	Selon le dernier Rapport de l'AEPD datant de 2011, l'agence emploie 154 fonctionnaires (la dotation étant de 157), 2 employés (la dotation étant de 7) et 1 haut fonctionnaire. Parmi ceux-ci, on compte 91 femmes et 69 hommes. En vertu de l'article 35.3 LO 15/99, les postes de travail des organes et des services qui font partie de l'AEPD sont assurés par des fonctionnaires des administrations publiques et par du personnel embauché à cet effet, selon la nature des fonctions assignées à chaque poste de travail. Les postes assignés aux fonctionnaires sont pourvus suivant la législation sur la fonction publique. Les postes des autres employés sont pourvus selon une procédure de recrutement publique respectueuse des principes d'égalité, mérite et capacité (article 37 du Statut). La priorité pour pourvoir des postes de travail revient aux fonctionnaires.

2.2. Komplexität und Zusammenwirken der Behörden

En vertu de l'article 35.1 LO 15/99 sur la protection des données, l'AEPD est une institution de droit public, dotée d'une personnalité juridique propre et de la capacité pour agir indépendamment, tant dans le domaine public que privé. Dans une décision du 30.11.2000[282], le Tribunal Constitutionnel a défini l'AEPD comme une institution spécialisée de droit public - qui a comme précédents de droit comparé les agences suédoise, allemande et française - investie des pouvoirs de contrôle sur les fichiers de données personnelles susceptibles de traitement automatisé.

Quant à la **position de l'AEPD**, l'article 35 de la LO 15/99 prévoit que dans l'exercice de ses fonctions, l'AEPD **agit indépendamment** des administrations publiques. L'AEPD est ainsi régie par la LO 15/99 et par un statut propre approuvé par le gouvernement (ci-après : le Statut)[283]. Dans l'exercice de ses fonctions publiques , à défaut de dispositions dans la LO 15/99 et dans son règlement d'application, l'AEPD doit agir en conformité avec la Loi 30/1992[284] sur le régime juridique des administrations publiques et la procédure administrative commune. Dans ses acquisitions patrimoniales et passations de marchés, elle est soumise au droit privé. Le Statut prévoit, à l'article 1.2, que le lien de l'AEPD avec le gouvernement est le Ministère de la justice.

Quant à son organisation, l'AEPD est une **entité publique** indépendante, qui possède des organes propres. En vertu de la LO 15/99, au sommet de la pyramide hiérarchique de l'AEPD se trouvent le **Directeur** et le **Conseil consultatif** (*Consejo consultivo*)[285] en dessous desquels on compte un

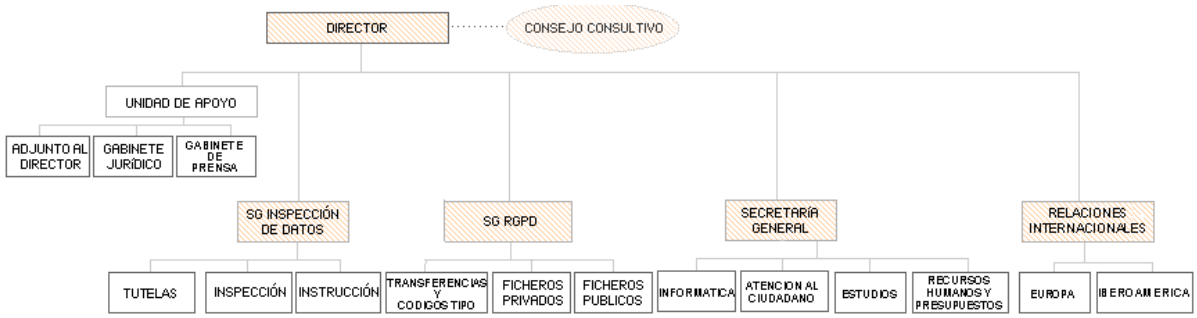
282 Tribunal Constitucional (Pleno), decisión del 30.11.2000, RTC 2000\290 (base privée).

283 Real Decreto 428/1993, de 26 de marzo, RCL 1993\1393 (base privée).

284 Ley 30/1992, de 26 de noviembre 1992, Administraciones publicas-procedimiento administrativo. Ley de Régimen Jurídico y Procedimiento Administrativo Común, RCL 1992\2512 (base privée).

285 Art. 11 DR 428/1993 Estructura orgánica.

Registre général de protection de données, une **Inspection** de données, un **Secrétariat** général et une **unité** de Relations internationales.



En vertu de la LO 15/99, les organes de l'AEPD sont le **Directeur** et le **Conseil consultatif** (*Consejo consultivo*)[286]. Il y a aussi un **Registre** général de protection de données, une **Inspection** de données et un **secrétariat** général. Selon le dernier Rapport de l'AEPD[287], l'agence emploie 154 fonctionnaires (la dotation étant de 157), 2 employés (la dotation étant de 7) et 1 haut fonctionnaire. Parmi ceux-ci, on compte 91 femmes et 69 hommes.

L'AEPD a pour tâche de **veiller à l'exécution et au respect de la législation sur la protection de données**. Le siège de l'AEPD se trouve à Madrid et sa sphère de compétences s'étend à toute l'Espagne. Toutefois, compte tenu du caractère **régionalisé** de l'Espagne et des compétences attribuées aux Communautés autonomes (CCAA) par la Constitution, certaines CCAA[288] ont constitué des autorités chargées d'agir dans ce même domaine. Il existe aussi des institutions qui agissent au niveau local.

Quant à la **répartition de tâches, l'**alinéa 2 de l'article 41 LO 15/99, dispose que les communautés autonomes peuvent créer et tenir leurs propres registres de fichiers pour l'exercice des compétences qui leur sont reconnues à l'égard de ces fichiers.

La Agencia Española de Protección de Datos se estructura en los siguientes órganos:
1. El Director de la Agencia Española de Protección de Datos.
2. El Consejo Consultivo.
3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

286 Art. 11 DR 428/1993 Estructura orgánica.
La Agencia Española de Protección de Datos se estructura en los siguientes órganos:
4. El Director de la Agencia Española de Protección de Datos.
5. El Consejo Consultivo.
6. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

287 Memoria AEPD 2011, disponible sous http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/Memoria_2011-ides-idphp.php (18.05.13).

288 Ceci est, par exemple, le cas de la Communauté de Madrid (Decreto 67/2003, de 22 de mayo LCM 2003\281, Aprueba el Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal), de la Catalogne (Decreto 48/2003, de 20 de febrero, Aprueba el Estatuto de la Agencia Catalana de Protección de Datos LCAT\2003\148), du Pays Basque (Ley 2/2004, de 25 de febrero LPV 2004\95, Comunidad Autónoma del País Vasco, Agencia Vasca de Protección de Datos y Regulación de Ficheros de Datos de Carácter Personal).

Le Décret Royal 428/1993 prévoit la participation de l'AEPD dans l'**élaboration et l'application des normes**. Pour ce faire, l'article 5[289] de ce texte dispose que l'AEPD collabore avec les organes compétents de l'État pour développer et appliquer des normes dans les matières visées par la LO 15/99. Dans ce cadre, l'AEPD émet des instructions et recommandations afin d'adapter le traitement automatisé de données aux dispositions de la LO 15/99 et d'appliquer les dispositions de ladite loi.

Dans une décision du 30.11.2000[290], Le Tribunal Constitutionnel a reconnu les compétences normatives (« potestad normativa ») de l'AEPD. Pour ce faire, le Tribunal a fait référence à l'article 37 c) et m) *in fine* LO 15/1999. En effet, l'art 37 c) LO 15/99 prévoit que l'AEPD est investie de la fonction de **définition des instructions** nécessaires pour rendre les traitements de données conformes aux principes de la LO 15/99. L'article 37 m) LO 15/99 dispose que l'AEPD **définira les instructions** nécessaires sur les conditions de sécurité des fichiers constitués à des fins exclusivement statistiques. Ce même point m) prévoit la compétence de l'AEPD pour l'exercice du pouvoir **exécutif** notamment pour sanctionner les infractions commises par les autres autorités publiques sur la base de l'article 46 LO 15/99[291]. En outre, l'article 41.1 LO 15/99 prévoit la **répartition des compétences** entre l'AEPD et les agences créées **dans le cadre des CCAA**. En application de cette disposition, les fonctions de protection des données sont exercées - lorsqu'elles se rapportent à des fichiers de données à caractère personnel créés ou gérés par les communautés autonomes sises dans leur domaine territorial - par les organes de chaque CCAA. Autrement dit, la ligne qui divise le champ des compétences de l'AEPD de celles des autorités des CCAA est la séparation entre les fichiers privés (qui sont de la compétence de l'AEPD) et les fichiers publics existant dans le cadre des CCAA (qui relèvent de la compétence de l'autorité régionale)[292]. Les organes régionaux chargés de la protection

---

289 Real Decreto 428/1993, de 26 de marzo - RCL\1993\1393, Art. 5 « Cooperación en la elaboración y aplicación de las normas. La Agencia de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la Ley Orgánica 5/1992, y a tal efecto:
a) Informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica.
b) Informará preceptivamente cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica.
c) Dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.
d) Dictará recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros ».

290 Tribunal Constitucional (Pleno), decisión del 30.11.2000, op. cit.

291 E. Puerto, La independencia de la Agencia Española de Protección de Datos: especial referencia a su potestad normativa, disponible sous www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142300901611&esArticulo=true&idRevistaElegida=1142302744259&language=es&pag=1&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales (14.04.13). Art. 46 LO 15/99 : « Infractions des administrations publiques. 1. Lorsque les infractions auxquelles se réfère l'article 44 ont été commises dans des fichiers publics ou concernant des traitements dont les responsables seraient responsables de fichiers de même nature, l'organe de sanction doit rendre une décision fixant les mesures qu'il y a lieu d'adopter pour la cessation desdites infractions ou la correction des effets de l'infraction. Cette décision est notifiée au responsable du fichier, à l'organe dont il dépend hiérarchiquement et aux personnes concernées, le cas échéant.
2. L'organe de sanction peut proposer également d'engager les actions disciplinaires, s'il y a lieu. La procédure et les sanctions à appliquer sont celles visées dans la législation sur le régime disciplinaire des administrations publiques.
3. Il convient de communiquer à l'organe de sanction les décisions rendues concernant les mesures et les actions
4. Le directeur de l'Agence doit communiquer au médiateur les actions qu'il a effectuées ainsi que les décisions rendues en vertu des paragraphes précédents » (traduction trouvée dans la Colección: Traducciones del derecho español
Edita: Ministerio de Justicia- Secretaría General Técnica, NIPO: 051-12-031-7 Traducción realizada por: Verbatim, S.A.), 2012.

292 M. Calderón, op. cit., p. 1838.

de données revêtent le caractère d'autorités de contrôle et jouissent d'une pleine indépendance et objectivité dans l'exercice de leur mission. De surcroît, et contrairement à l'ancienne loi sur la protection de données (qui était en vigueur avant la promulgation de la LO 15/99), l'article 41 LO 15/99 prévoit expressément que les administrations locales peuvent créer et gérer des fichiers de données à caractère personnel. L'article 41 LO 15/99 prévoit certaines exceptions, notamment pour le domaine des transferts internationaux de données (points j), k) et l), et les points f) et g) de l'article 37 LO 15/99[293]). Une autre exception sont les compétences concernant le traitement d'infractions commises par les responsables des administrations publiques[294] ainsi que les pouvoirs relatifs à l'immobilisation de fichiers (articles 46 et 49 LO 15/99).

Le Directeur de l'AEPD peut convoquer régulièrement les organes correspondants des CCAA aux fins de coopération institutionnelle et de coordination des critères ou des procédures d'action. Le Directeur de l'AEPD et les organes correspondants des CCAA peuvent solliciter mutuellement l'information nécessaire à l'accomplissement de leurs fonctions. Dans tous les cas, il faut tenir compte du fait que la distribution de compétences doit suivre ce qui est prescrit par la Constitution espagnole, principalement à l'article 149.1.1, d'après lequel il appartient en exclusivité à l'État central de régler les conditions de base garantissant l'égalité des espagnols dans l'exercice de leurs droits et dans l'accomplissement de leurs obligations. Les CCAA qui n'ont pas assumé de compétences en matière de protection de données, restent soumises à la législation de l'État Central. En revanche, les CCAA qui ont assumé de telles compétences, possèdent des pouvoirs législatifs par rapport à l'exécution du droit fondamental de la protection des données dans leur territoire, à condition de ne pas empiéter sur le domaine de base qui reste réservé à l'État central[295].

Le **Directeur** de l'AEPD est à la tête de l'Agence et exerce sa représentation (article 36 LO 15/99). Il exerce sa fonction en toute indépendance et objectivité, **n'étant soumis à aucune instruction** dans l'exercice de ses fonctions. Il est nommé par décret royal parmi les membres du conseil consultatif, pour une période de quatre ans.

Les membres du **Conseil consultatif** de l'AEPD sont nommés par le gouvernement sur proposition préalable par les diverses entités publiques faite au Ministère de la justice. Le Conseil consultatif de l'AEPD est composé de la façon suivante :

---

293 Il s'agit des fonctions suivantes : f) requérir des responsables et des personnes chargées des traitements, après audience, qu'ils prennent les mesures nécessaires à la mise en conformité du traitement des données à la loi et, le cas échéant, ordonner la cessation des traitements et l'annulation des fichiers en cas de non-conformité; g) exercer le pouvoir de sanction; j) assurer la publicité de l'existence des fichiers de données à caractère personnel; k) rédiger un mémoire annuel et l'adresser au Ministère de la Justice;
l) exercer le contrôle et accorder les autorisations pertinentes en rapport avec les flux internationaux de données ainsi qu'exercer les fonctions de coopération internationale en matière de protection des données à caractère personnel.

294 E. Puerto, op. cit., « Asimismo, corresponde a la Agencia ejercer la potestad a la que se refiere el artículo 46 de la LOPD, en relación con las infracciones de las Administraciones Públicas, de tal modo que cuando las infracciones comprendidas en el artículo 44 de dicha Ley Orgánica sean cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia Española de Protección de Datos **dictará una resolución** estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera ».

295 E. Román & J. Mora, Un análisis de la estructura institucional de protección de datos en España, un análisis jurídico y económico de la incidencia de las autoridades de control españolas en la garantía del derecho fundamental de autodeterminación informativa, barcelona 2009, p. 13 disponible sous http://www.indret.com/pdf/641_es.pdf (16.04.13).

a. le Congrès des députés désigne un membre (un député),
b. le Sénat désigne un membre (un sénateur),
c. le Ministre de la justice désigne un membre appartenant à l'administration de l'État,
d. les Communautés autonomes désignent un membre par décision prise à la majorité,
e. la Fédération espagnole des municipalités et des provinces désigne un membre de l'administration locale,
f. l'Académie royale d'histoire désigne un membre appartenant à celle-ci,
g. le Conseil des universités désigne un membre expert dans le traitement de données automatisées,
h. le Conseil de consommateurs et usagers désigne un membre,
i. le Conseil supérieur des Chambres de commerce, de l'industrie et de la navigation désigne un membre.

Les membres choisis par ces entités sont présentés au gouvernement par le Ministère de la justice. La durée de leur mandat est de quatre ans.

Le Directeur doit entendre le Conseil consultatif concernant les propositions qui lui sont faites par ce dernier dans l'exercice de ses fonctions. Le Directeur peut cesser d'exercer ses fonctions avant l'expiration de la période fixée, à sa propre demande ou pour cause de révocation décidée par le gouvernement, après instruction du dossier, procédure au sein de laquelle sont nécessairement entendus les autres membres du Conseil consultatif. Une telle situation peut se rencontrer en cas d'inexécution grave par le Directeur de ses obligations, d'incapacité pour l'exercice de sa charge, incompatibilité ou condamnation pour dol.

Dans le cadre de l'exercice de ses pouvoirs, le **Directeur** peut, à tout stade, exiger qu'il soit mis fin à l'utilisation ou à la cession illicite des données appartenant à un fichier. Cette compétence concerne tant les fichiers publics que privés. Si la demande n'est pas respectée dans les trois jours, le Directeur peut – par décision motivée – ordonner l'immobilisation du fichier. Un autre pouvoir du Directeur est celui d'autoriser la réalisation de visites sur place par des inspecteurs de l'AEPD afin d'examiner des fichiers. Le Directeur prend, en cas d'infraction constatée, une résolution visant à initier la procédure de sanction. Le Directeur a aussi des compétences pour sanctionner les actes contraires à la loi sur la protection de données en ordonnant, si nécessaire, la prise de mesures provisoires.
Finalement, le **Directeur** possède des compétences dans le cadre du transfert international de données : il autorise le transfert par la voie d'une décision.

Parmi les critères assurant **l'indépendance** de l'AEPD et les mesures de précaution pour consolider l'indépendance on peut nommer les points suivants :

- Organisation non-dépendante d'un autre pouvoir
- institutions propres
- statut propre
- pouvoir normatif
- gestion indépendante du budget
- compétence pour imposer des sanctions et prendre des mesures provisoires

Même si le Conseil consultatif de l'AEPD est constitué notamment d'un député, un sénateur, un membre des CCAA et un membre de l'administration de l'État nommé par le ministre de la justice, **il n'est pas possible d'affirmer que l'AEPD représente des groupes d'intérêt politique**.

Pour ce qui concerne les **avantages et désavantages du système, l**a doctrine[296] souligne que, d'un côté, le système de protection de données espagnol a une structure assez complexe, notamment en raison des développements d'entités au niveau régional et local et des problèmes de coordination et conflits de compétences. La complexité constatée dans la distribution des compétences (qui a conduit à l'intervention du Tribunal Constitutionnel[297]) peut causer un manque de clarté au sens où les citoyens et entreprises ne savent pas à quelle autorité ils doivent s'adresser dans des cas précis. En revanche, en ce qui concerne l'effectivité de ce système, on constate que lorsqu'il existe une agence régionale de protection des données, la quantité de fichiers contrôlés dans la région augmente considérablement. C'est aussi le cas des dénonciations et des consultations de la part des citoyens et entreprises. Autrement dit, la multiplicité d'entités semble renforcer – dans le cadre de leurs interventions conjointes – la protection des données.

296 E. Román & J. Mora, op. cit. , p. 28.

297 Tribunal Constitucional (Pleno), decisión del 30.11.2000, op. cit.

3. Behördenmitglieder und Mitarbeitende

3.1. Übersicht

Ernennung der Behördenmitglieder	Le Directeur de l'AEPD est nommé par décret royal parmi les membres du conseil consultatif.
Persönliche und fachliche Anforderungen der **Behördenmitglieder** und Mitarbeitenden	Le Directeur est choisi parmi les membres du Conseil consultatif de l'AEPD (les membres du Conseil consultatif sont un sénateur, un membre de l'administration de l'État, un membre représentant les régions, un membre de la fédération de municipalités et provinces, un membre de l'Académie de l'histoire, un membre des académies universitaires, un membre proposé par les Chambres de commerce, industrie et navigation). Le Directeur est soumis aux mêmes incompatibilités que les autres titulaires de hautes charges de l'État sur la base de la loi 9/1991, de 22 mars 1991.
Ausgestaltung des Arbeitsverhältnisses	Le Directeur de l'AEPD remplit une haute chargede l'État. Il doit être placé ensituation de services spéciaux en cas d'exercice préalable d'une fonction publique. Il en va de même en cas d'exercice préalable d'une fonction relevant de la carrière judiciaire ou du ministère public. Le Directeur peut être révoqué par le gouvernement, après une instruction du dossier au cours de laquelle sont nécessairement entendus les membres du Conseil consultatif, en cas d'inexécution grave de ses obligations, d'incapacité pour l'exercice de sa charge, incompatibilité ou condamnation pour dol.
Zulässigkeit der **Nebenbeschäftigungen**	La personne nommée pour diriger l'AEPD qui exerce une fonction administrative publique ou qui est magistrat ou encore membre du ministère public, doit être placée en situation administrative de services spéciaux. Elle est soumise aux mêmes incompatibilités que les autres personnes remplissant de hautes charges de l'État. En vertu de l'art. 2 de la Loi 5/2006, le Gouvernement, préalablement à la nomination du Directeur, informera le Parlement du nom du candidat afin de prévoir qu'il puisse comparaître devant une commission parlementaire. La Commission émettra alors un Avis quant à l'existence ou non d'incompatibilités.
Regelungen über Voll- bzw. Teilzeitarbeit bei der obersten Führungsstufe	Le poste du Directeur est à temps complet
Länge der Amtsdauer	Le Directeur est nommé pour une période quadriennale.

3.2. Nebenbeschäftigungen und Teilzeitarbeit insbesondere

Nous n'avons pas trouvé d'informations quant à l'admissibilité d'activitéss accessoires. Nous avons contacté l'AEPD mais aucune réponse ne nous est parvenue à ce jour.

3.3. Die Entlöhnung insbesondere

Nous n'avons pas trouvé d'informations portant sur la question de savoir si la rémunération est regardée comme étant raisonnable.

4. Unabhängigkeit und Umgang mit Interessenkonflikten

Unabhängigkeit der Behörde und deren Mitglieder und Mitarbeitenden	L'article 35 LO 15/99 dispose que l'AEPD est un organisme de droit public, doté d'une personnalité morale propre et d'une pleine capacité publique et privée, qui agit indépendamment des administrations publiques dans l'exercice de ses fonctions. L'AEPD agit sur la base d'un statut propre approuvé par le gouvernement. Le directeur de l'AEPD est à la tête de l'Agence et peut la représenter (art. 36 LO 15/99). Il exerce sa fonction en toute indépendance et objectivité, n'étant soumis à aucune instruction dans l'exercice de ses fonctions. L'AEPD ne représente pas des personnes ou des intérêts politiques. Les organes régionaux chargés de la protection de données revêtent le caractère d'autorités de contrôle et jouissent d'une pleine indépendance et objectivité dans l'exercice de leur mission.
Möglichkeit der **Weisungen von aussen**	Le Directeur n'est soumis à aucune instruction externe.
Neutralität der Behörde	Il n'y a pas de dispositions visant spécifiquement à sauvegarder la neutralité, mais la structure interne de l'AEPD et la façon dont les membres de ces organes sont désignés ainsi que la large indépendance accordée à l'AEPD semblent contribuer à garantir la neutralité.

5. Ressourcen

5.1. Übersicht

Budgethoheit	L'AEPD élabore et approuve chaque année l'avant-projet de son budget annuel et l'adresse au gouvernement pour qu'il soit incorporé au budget général de l'État (*presupuestos generales del Estado*), en tant qu'élément indépendant.
Einnahmequellen der Behörde	Pour l'accomplissement de ses objectifs, l'AEPD compte avec les biens et moyens suivants: a) les assignations fixées (annuellement) à la charge du budget général de l'État; b) les biens et les valeurs qui constituent son propre patrimoine, ainsi que les produits et les revenus de ceux-ci. En application de l'article 35.2 LO 15/99, les acquisitions de patrimoine par l'AEPD sont sujettes au droit privé. Toutefois, en vertu de la promulgation d'une législation postérieure qui règle les contrats de l'administration publique, la doctrine estime que ces contrats sont aujourd'hui soumis au régime de la nouvelle législation.c) tous autres moyens pouvant lui être attribués légalement.
Verfügt die Behörde **über ein eigenes Budget.**	Oui. L'AEPD élabore et approuve chaque année l'avant-projet de son budget annuel et l'adresse au gouvernement pour qu'il soit incorporé au budget général de l'État, en tant qu'élément indépendant.

5.2. Adäquanz des Budgets insbesondere

Un auteur souligne que le rôle de l'AEPD – qui peut être jugé de « correct » - sera amélioré lorsque le public sera plus conscient de ses droits et lorsque les responsables du traitement connaîtront mieux leurs obligations. La procédure d'imposition de sanctions ne suffit pas pour créer une telle conscientisation. Afin de remplir ces tâches, il propose d'augmenter le budget de l'AEPD au même niveau que le budget d'agences similaires en Europe[298]. Il est aussi suggéré qu'une majeure décentralisation des tâches de l'AEPD, par exemple, en attribuant plus de compétences aux entités régionales, aura pour effet d'étendre la connaissance des droits et devoirs en vertu de la loi sur la protection des données en Espagne.

[298] I. Gómez-Suarez, Estudio del régimen sancionador de la Ley Orgánica 15/1999, Revista Española de Protección de Datos, n° 4, 2008, p. 189.

6. Aufgabenerfüllung

6.1. Übersicht

Zugänglichkeit der Behörde für die Betroffenen (andere Behörden, Unternehmen, Privatpersonen)	L'AEPD a pour fonction, entre autres, celle de répondre aux demandes et réclamations formulées par les personnes concernées et celle d'informer les personnes sur leurs droits en matière de traitement des données à caractère personnel. La LO 15/99 prévoit le droit d'accès à l'autorité par des entreprises, individus et d'autres autorités. Les principaux domaines concernés sont les suivants : **Droit de connaître l'existence de traitements de données**. Toute personne peut connaître, en obtenant à cet effet l'information opportune auprès du Registre général de protection des données, l'existence de traitements de données à caractère personnel, leurs finalités et l'identité du responsable du traitement. La consultation du registre général est publique et gratuite **(article 14 LO 15/99).** **Protection de droits.** Les actions contraires aux dispositions sur la protection de données espagnoles, peuvent faire l'objet d'une réclamation par les intéressés auprès de l'AEPD. Notamment, l'intéressé auquel il est refusé, totalement ou partiellement, l'exercice des droits d'opposition, d'accès, de rectification ou d'annulation, peut en informer l'AEPD ou, le cas échéant, l'organisme compétent au sein de chaque CCAA, qui doit vérifier le caractère opportun ou non du refus. Le délai maximal pour rendre la décision expresse de tutelle des droits est fixé à six mois. En vertu de l'article 18 LO 15/99, il est possible de faire recours à l'encontre des décisions de l'AEPD auprès du tribunal du contentieux administratif. Lorsqu'un intéressé demande le droit d'accès au responsable d'un fichier et celui-ci rejette la demande, il doit informer l'intéressé de son droit de solliciter la protection de l'AEPD ou d'une agence régionale[299]. Outre la violation des lois sur la protection des données, chacun peut procéder à une dénonciation auprès de l'AEPD suite à la réception non-sollicitée de communications commerciales électroniques[300]. Afin de faciliter l'accès à cette procédure, l'AEPD propose un formulaire en ligne[301]. **Fichiers des CCAA.** Lorsque le Directeur de l'AEPD constate que la maintenance ou l'utilisation d'un fichier donné des CCAA enfreint une disposition de la LO 15/99 en matière de compétences exclusives, il peut requérir à l'administration correspondante d'adopter les mesures correctrices déterminées dans un

299 Art. 30.3 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13.12.1999 (RCL 1999\3058), de protección de datos de carácter personal, Real Decreto 1720/2007, de 21.12.07.

300 Ces compétences sont attribuées à l'AEPD par les articles 35.3 et 43 de la Loi 34/2002 sur les Services de la société d'information et de commerce électronique et l'article 58 de la Loi 32/2003 dite loi générale sur les télécommunications.

301 Le formulaire de dénonciation en ligne est disponible sous : https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaDenuncia/nuevaDenuncia.jsf (13.04.13).

	délai explicitement fixé dans la requête (article 42 LO 15/99).
Möglichkeiten der Behörde zur Durchsetzung ihrer Kompetenzen	L'AEPD peut prendre des mesures dans différents domaines. Par exemple, en vertu de l'article 121 du Real Decreto 1720/2007, du 21 décembre 2007 (ci-après : RD 1720), le **Directeur** peut- à tout stade des procédures – demander qu'il soit mis fin à l'utilisation ou à la cession illicite des données appartenant à un fichier. Cette compétence concerne tant les fichiers publics que privés. S'il n'est pas satisfait à la demande dans un délai de trois jours, le Directeur peut - par décision motivée – ordonner l'immobilisation du fichier. Les **inspecteurs** de l'AEPD sont compétents pour collecter des informations. Pour ce faire, ils peuvent exiger l'accès à des documents et données pour les examiner. Ils peuvent aussi accéder aux lieux où des programmes et traitements et supports sont installés (art. 124 DR 1720). En outre, les inspecteurs sont compétents, après avoir été autorisés par le Directeur, pour réaliser des visites sur les lieux où se trouvent des fichiers. A l'issue des procédures préalables, si des indices d'infraction sont constatés, le Directeur de l'AEPD prend une décision pour initier la procédure de sanction (art. 126 RD 1720). L'AEPD, dans la personne du **Directeur,** est aussi compétente pour sanctionner les actes contraires à la loi sur la protection de données. Le Directeur peut, le cas échéant, prendre les mesures provisoires nécessaires. Finalement, la LO 15/99 octroie des compétences au **Directeur** dans le cadre du transfert international de données. Il autorise le transfert par la voie d'une décision (*resolución*), qui est ensuite transmise au Registre général de la protection de données afin de procéder à l'inscription et au Ministère de la justice afin de notifier la Commission européenne et les États membres conformément à ce qui est prévu à l'article 26.3 de la Directive 95/46/CE. Le cas échéant, le Directeur est aussi compétent pour adopter une décision d'interruption du transfert international de données.
Weitere Aufgaben der Datenschutzbehörde	Outre la violation des lois sur la protection des données, chacun peut présenter une dénonciation auprès de l'AEPD suite à la réception non-sollicitée de communications commerciales électroniques. Afin de faciliter l'accès à cette procédure, l'AEPD propose un formulaire en ligne.

6.2. Kompetenzen der Behörde

Le **Directeur** peut, à tout stade, exiger qu'il soit mis fin à l'utilisation ou à la cession illicite des données appartenant à un fichier. Cette compétence concerne tant les fichiers publics que privés. Si la demande n'est pas respectée dans les trois jours, le Directeur peut - par décision motivée – ordonner l'immobilisation du fichier.

Le Directeur peut également autoriser la réalisation de visites sur place par des inspecteurs de l'AEPD afin d'examiner des fichiers.

En outre, en cas d'infraction constatée, le Directeur prend une décision visant à initier la procédure de sanction.

Le Directeur est aussi compétent pour sanctionner les actes contraires à la loi sur la protection de données en ordonnant, si nécessaire, la prise de mesures provisoires.

Finalement, le **Directeur** possède des compétences dans le cadre du transfert international de données : il autorise le transfert par la voie d'une décision.

6.3. Akzeptanz und Ansehen

Un auteur[302] souligne que la réputation de l'AEPD est „correcte", même si elle peut faire l'objet d'améliorations. Par exemple, d'après cet auteur, il conviendrait d'endiguer les activités qui consistent à proposer à des entrepreneurs, en échange d'honoraires, des services de vérification de la conformité de leurs bases de données aux normes de la loi. Il n'y a rien d'illégal dans une telle activité, mais l'auteur se pose la question de savoir si l'objectif de la LO 15/99 était celui de promouvoir la création de telles activités lucratives. La situation devient d'autant plus manifeste avec la création de programmes spécifiques d'assurance proposés à ceux qui risquent de se voir sanctionnés par l'AEPD.

En général, afin de faciliter l'adaptation de la loi sur la protection des données aux changements rapides de la société, il est proposé de ne pas maintenir la législation dans ce domaine dans une loi organique (nécessitant une majorité qualifiée pour sa modification).

6.4. Evaluation einer allfälligen Doppelrolle (Datenschutz und Öffentlichkeitsprinzip)

n/a

302 I. Gómez-Juarez, op. cit., p. 189.

IV. SCHLUSSFOLGERUNG

Alle analysierten Staaten haben eine staatliche **Kontroll- und Aufsichtsbehörde**, die für die allgemeine Überwachung der Anwendung der datenschutzrechtlichen Bestimmungen und die Sicherstellung ihrer Befolgung im jeweiligen Hoheitsgebiet zuständig ist. Mehrere Mitgliedstaaten (z.B. die Niederlande) haben eine Datenschutzbehörde mit allgemeiner Zuständigkeit und mehrere weitere, spezifische Kontrollstellen eingerichtet (vgl. z.B. Deutschland, Finnland). Manche Staaten mit föderaler oder regionaler Organisation (z.B. Deutschland oder Spanien) wiederum haben eine staatliche Kontrollstelle und mehrere Kontrollstellen mit entsprechender Funktion auf regionaler oder teilstaatlicher Ebene eingerichtet. Da zudem in manchen Ländern (z.B. in Schweden, Finnland, Slowenien) vor der Einrichtung von Datenschutzbehörden die Zuständigkeit für den Schutz des Rechts auf Privatsphäre bei behördlichen Bürgerbeauftragten lag, kommt in manchen Mitgliedstaaten (z. B. in Finnland, Slowenien) weiterhin dem Bürgerbeauftragten massgebliche Bedeutung für den Schutz personenbezogener Daten zu. Allerdings scheint unserer Meinung nach eine übermässig grosse Anzahl an Datenschutzorganen und -stellen für eine Sensibilisierung der Bürger für die Existenz solcher Stellen nicht erforderlich. Zudem führt eine Vielzahl von Organen zu Unübersichtlichkeit und unnötiger Komplexität.

Die untersuchten Staaten bemühen sich, dass ihre nationalen Datenschutzbehörden die ihnen zugewiesenen Aufgaben in völliger **Unabhängigkeit** wahrnehmen. In mehreren Staaten (z.B. in Deutschland, Italien, Polen und in Slowenien) werden Datenschutzbeauftragte durch die gesetzgebende Versammlung gewählt, zuweilen sogar im Wege von Verfahren, die einen Konsens zwischen der Mehrheit und der Opposition erfordern. Mit wenigen Ausnahmen stellt dies ein hohes Mass an Unabhängigkeit der gewählten Mitarbeiter sicher. In verschiedenen Mitgliedstaaten dagegen werden Datenschutzbeauftragte ohne Beteiligung der parlamentarischen Opposition direkt von der Regierung ernannt (z.B. Schweden, Finnland, Vereinigtes Königreich oder Niederlande). Verschiedentlich hat dies zu Bedenken hinsichtlich der tatsächlichen Unabhängigkeit der Datenschutzbehörde geführt. Zu ähnlichen Bedenken kann es in Ländern kommen, in denen die Kontrollstelle dem Justizministerium angegliedert ist (z.B. Schweden, Finnland, das Vereinigte Königreich). Andere Staaten (z.B. Frankreich, Spanien) schliesslich sehen für die Berufung der Datenschutzbeauftragten ein kombiniertes Verfahren vor, an dem zugleich die Exekutive, die Legislative und die Judikative oder andere organisierte gesellschaftliche Gruppen mitwirken. In Italien haben Mitarbeiter von Datenschutzbehörden eine Amtszeit von sieben Jahren, wobei eine Amtsenthebung oder erneute Berufung für eine zweite Amtszeit untersagt ist. In manchen Ländern (z.B. in Polen und Slowenien) können Mitarbeiter von Datenschutzbehörden nur bei besonderem Fehlverhalten und nur unter Einhaltung des gleichen Verfahrens, das auch bei ihrer Berufung zur Anwendung gekommen ist, vorzeitig ihres Amtes enthoben werden. In anderen Staaten sind die Datenschutzbeauftragten-Amtszeit auf vier (Polen), fünf (Deutschland, Frankreich, Finnland), sechs (Niederlande) und sieben (Vereinigtes Königreich) Jahre gesetzt, wobei eine einmalige Wiederberufung möglich ist. Diese technischen Lösungen gewährleisten ein gewisses Mass an Unabhängigkeit der Kontrollstellen, indem die Einflussnahme und der Druck der politischen Kräfte gemindert werden. Die Autonomie der Kontrollstelle wird besonders gestärkt, wenn die Existenz und der Aufgabenbereich einer unabhängigen, mit der Kontrolle der Einhaltung der Datenschutzbestimmungen beauftragten Behörde explizit in der Verfassung verankert sind. Für weitere wichtige Garantien hinsichtlich der institutionellen Unabhängigkeit wird dann gesorgt, wenn die Datenschutzbehörde eine eigene Rechtspersönlichkeit erhält (z.B. in Polen und Slowenien) und ihr die Möglichkeit eingeräumt wird, Gerichtsverfahren vor dem einzelstaatlichen Verfassungsgericht anzustrengen (wie in Slowenien).

In den meisten untersuchten Staaten erhalten die Datenschutzbehörden die für ihre Funktion nötigen **Ressourcen** aus dem Staatshaushalt (z. B. Deutschland, Frankreich, Italien, Polen, Slowenien), häufig aus dem Haushalt des Justizministeriums (z.B. in den Niederlanden). In manchen

Staaten können die Kontrollstellen ihre finanziellen Ressourcen jedoch durch die Einnahmen aus den Meldungen der Datenverarbeiter und/oder durch die bei Verstössen gegen Datenschutzbestimmungen verhängten finanziellen Sanktionen erheblich erhöhen (z.B. in Schweden und Finnland). Im Vereinigten Königreich sind Meldegebühren die einzige Einnahmequelle für die Datenschutztätigkeit der Kontrollstelle. In einigen Staaten (insbesondere z.B. in Frankreich, Italien) wurden Probleme in Bezug auf unzureichende Finanzausstattung der Kontrollstellen hervorgehoben. In anderen Ländern, in denen die Datenschutzbehörde derzeit finanziell relativ gut ausgestattet ist, sind für die kommenden Jahre mögliche Haushaltskürzungen zu erwarten (z.B. in Spanien).

Generell können bei der Analyse der **Befugnisse** der verschiedenen nationalen Datenschutzbehörden zwei allgemeine Tendenzen unterschieden werden, in denen die Konzepte zum Ausdruck kommen, die die Mitgliedstaaten bei der Umsetzung des Datenschutzes anwenden. Während mehrere Länder (z.B. Deutschland, Finnland, Schweden und das Vereinigte Königreich) die **präventive und proaktive** Rolle der Kontrollstellen betont haben, indem sie den Schwerpunkt auf deren Ex-ante-Rolle bei der Gewährleistung des Schutzes personenbezogener Daten gelegt haben, haben andere Mitgliedstaaten (z.B. Frankreich, Polen) der **Ex-post-Durchsetzungs- und Kontrollfunktion** der Datenschutzbehörden Priorität gewährt und diesen eine reaktive Pflicht zur Überwachung der Einhaltung der Datenschutzbestimmungen übertragen. Entsprechend unterscheidet sich die Art der den Kontrollstellen übertragenen Befugnisse, wobei entweder „weichen" Präventionsinstrumenten in den erstgenannten Fällen bzw. „härteren" Massnahmen in den letztgenannten Fällen der Vorzug gegeben wird. Es gibt auch Länder (z.B. Italien, die Niederlande und Slowenien), die einen Mittelweg eingeschlagen haben, indem sie ihren nationalen Datenschutzbehörden Befugnisse zur aktiven Unterstützung und Gewährleistung der Einhaltung der Datenschutzbestimmungen übertragen und sie gleichzeitig zur Verfolgung und Bestrafung von Verstössen ermächtigt haben.

Datenschutzbehörden verfügen in allen untersuchten Rechtsordnungen über **Untersuchungsbefugnisse**, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen. So sind die Datenschutzbehörden befugt, die Einhaltung der Datenschutzbestimmungen durch private und öffentliche Datenverarbeiter zu überwachen und insbesondere bei den Beteiligten Kontrollen durchzuführen, Untersuchungen vorzunehmen, die Erteilung von Informationen anzuordnen, die Gewährung des Zugangs zu geschäftlichen Daten und Unterlagen anzuordnen sowie Daten und Unterlagen zu kopieren. Diese Befugnisse können von Amts wegen oder auf Ersuchen oder Antrag einer betroffenen Person, die Verstösse gegen ihre Rechte im Zusammenhang mit ihren personenbezogenen Daten geltend macht, ausgeübt werden. Die Kontrollstellen können im Rahmen der Ausübung ihrer Funktionen und zur Aufdeckung von Verstössen gegen die Datenschutzbestimmungen Räumlichkeiten und etwaige sonstige Orte, an denen eine Datenverarbeitung erfolgt, betreten, die nötige Ausrüstung beschlagnahmen, Untersuchungen durchführen und Beweismittel an sich nehmen; diese Möglichkeit besteht im Prinzip auch ohne Zustimmung des für die Datenverarbeitung-Verantwortlichen und ohne eine vorherige richterliche Anordnung.[303]

In gewissen Staaten (z.B. in Frankreich, Niederlande, Polen, Slowenien, im Vereinigten Königreich) verfügen die Behörden über teilweise weitgehende Befugnisse, mit welchen die Datenbearbeitung in konkreten Fällen beeinflusst wird. Eine erste Massnahme ist beispielsweise die Möglichkeit, vor der Durchführung der Verarbeitung sensibler Daten Gutachten abzugeben und für eine geeignete **Veröffentlichung** der Gutachten zu sorgen. Wesentlicher eingreiffender ist die Befugnis, die

303 Allerding mit einigen Ausnahmen. Z.B. in Deutschland können sie alleine weder die Sperrung, Löschung oder Vernichtung von Daten anordnen noch ein vorübergehendes oder endgültiges Verarbeitungsverbot verhängen. Im Vereinigten Königreich und in Frankreich haben sie ohne vorherige richterliche Anordnung keinen Zutritt zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden.

Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen. Als Mittellösung zwischen diesen beiden Formen findet sich auch die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten.

Alle Kontrollstellen sind verpflichtet, ein **Register der Meldungen der Datenverarbeitungen** zu führen. Sie können zudem anordnen, dass ein privater für die Verarbeitung Verantwortlicher eine gegen die Datenschutzbestimmungen verstossende Datenverarbeitung abbricht und spezifische Daten, die Gegenstand einer solchen Verarbeitung sind, berichtigt, löscht oder sperrt. Die Kontrollstellen können weiter den privaten für die Verarbeitung Verantwortlichen die Nutzung eines festgelegten Verfahrens in Verbindung mit der Datenverarbeitung untersagen, wenn ein erhebliches Risiko besteht, dass Daten unter Verstoss gegen die geltenden Rechtsvorschriften verarbeitet werden und können auch anordnen, dass private für die Verarbeitung Verantwortliche spezifische technische und organisatorische Sicherheitsmassnahmen durchführen müssen, die für den Schutz gegen die zufällige oder unrechtmässige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die Weitergabe an unbefugte Personen, den Missbrauch von Daten und andere Formen der unrechtmässigen Verarbeitung von Daten erforderlich sind.

Alle Kontrollstellen haben auch die Befugnis zur **Befassung mit Eingaben von Beteiligten**, die einen Verstoss gegen ihre Rechte im Zusammenhang mit ihren personenbezogenen Daten geltend machen, und sind dementsprechend verpflichtet, dem Beschwerdeführer innerhalb einer festgelegten Zeit eine Antwort zukommen zu lassen. Erweist sich eine Eingabe am Ende einer Untersuchung als begründet, können allerdings wenige nationale untersuchte Datenschutzbehörden eigenständig ein Gerichtsverfahren vor einem zuständigen Gericht anstrengen (in Slowenien ist es möglich sogar vor dem Verfassungsgericht), oder unmittelbar eine quasirichterliche Funktion übernehmen und unmittelbar über die Eingabe des Klägers entscheiden (als alternatives Forum zu ordentlichen Gerichten). Entscheidungen der administrativen Kontrollstellen mit quasirichterlichen Befugnissen sind in jedem Fall stets vor ordentlichen Gerichten anfechtbar.

Datenschutzbehörden haben überall die quasi-legislative Befugnis, **allgemeine Rechtsverordnungen für spezifische Sektoren zu erarbeiten**, die Ausarbeitung privater Verhaltenskodizes zu fördern und Gutachten und Empfehlungen für im Bereich des Datenschutzes tätige öffentliche und private Akteure abzugeben. Diese Massnahmen sind jedoch **meist nicht rechtsverbindlich**. Gleichzeitig gestehen viele Staaten den Kontrollstellen bei der Beratung der Exekutive und der Legislative im Hinblick auf Gesetzesvorlagen zum Schutz personenbezogener Daten eine Konsultativfunktion zu. Ihre Ratschläge zu Gesetzesvorlagen und Verordnungsentwürfen sind daher optional oder (wie in Deutschland, Frankreich, Italien) nur bei der Ausarbeitung von Durchführungsvorschriften rechtlich absolut erforderlich.[304]

Die **Zusammenarbeit** und die regelmässige Kommunikation nationaler Datenschutzbehörden mit anderen staatlichen Stellen könnten zu einem reibungsloseren Funktionieren des Datenschutzsystems insgesamt beitragen. Gewisse potenzielle Defizite verbleiben: Auf **struktureller Ebene** ist die

---

304 Das Fehlen von Gutachten der Datenschutzbehörden vor der Inkraftsetzung von Rechtsvorschriften oder Rechtsverordnungen, die möglicherweise nachteilige Auswirkungen auf den Schutz personenbezogener Daten haben können, kann jedoch ein Anzeichen dafür sein, dass der Bedeutung des Schutzes der Privatsphäre bei politischen Entscheidungen nicht in vollem Umfang Rechnung getragen wird. In vielen Ländern (z. B. in Frankreich, Italien, Polen, Slowenien, sowie im Vereinigten Königreich) wiederum werden Kontrollstellen vom Gesetzgeber bei der Ausarbeitung von Gesetzen, die sich auf die Privatsphäre und den Datenschutz auswirken können, nur willkürlich konsultiert, weil keine konkrete entsprechende Verpflichtung für den Gesetzgeber besteht.

mangelnde Unabhängigkeit verschiedener Datenschutzbehörden hervorzuheben (z.B. Vereinigtes Königreich und Finnland). In einigen Staaten (z.B. in Italien) bestehen Bedenken dahingehend, dass die Mitarbeiter von Datenschutzbehörden ihre Aufgaben möglicherweise nicht genug effizient und in völliger Unabhängigkeit erfüllen können. In diesen Rechtsordnungen liegen normative oder praktische Hindernisse vor, welche zu Zweifeln hinsichtlich der tatsächlichen Unabhängigkeit nationaler Datenschutzbehörden von der staatlichen Politik Anlass geben.

Die Unabhängigkeit wird in erster Linie durch das Verfahren zur Benennung und Abberufung von leitenden Mitarbeitern der Datenschutzbehörden gewährleistet. In einigen Staaten werden Datenschutzbeauftragte unter Ausschluss der parlamentarischen Opposition direkt von der Regierung benannt (z.B. Niederland oder Schweden). Wenn die ausschliessliche Befugnis zur Auswahl bei der Regierung liegt und Vorschläge, Nachprüfungen oder Zustimmungen des Gesetzgebers nicht vorgesehen sind, erhöht sich die Gefahr einer faktischen Subordination oder Marginalisierung der Kontrollstellen. Ähnliche Probleme könnten sich u. E. daraus ergeben, in denen die Überwachungsbehörde dem Justizministerium zugeordnet ist (z.B. Finnland, Schweden). Je nach Ausgestaltung könnte die Regierung bei einer Zuordnung de facto direkt oder indirekt die Mehrheit der benannten Mitarbeiter kontrollieren und damit letztlich den Zweck eines pluralistischen Benennungsverfahrens unterlaufen. Anzeichen einer solchen Beeinflussung haben sich in den betroffenen Staaten allerdings nicht gefunden. Ebenfalls zur Gewährung der formellen Unabhängigkeit geeignet scheint ein kombiniertes Verfahren zur Benennung der Mitarbeiter der nationalen Datenschutzbehörden wie in Spanien, an dem die Exekutive, die Legislative und die Judikative bzw. sonstige organisierte Gruppen der Gesellschaft gleichzeitig beteiligt sind.

Die Unabhängigkeit der Datenschutzbehörden ist ein unverzichtbarer Faktor für die Gewährleistung eines hohen Masses an Datenschutz. Unter diesem Gesichtspunkt können strukturelle Massnahmen wie die Verleihung einer eigenen Rechtspersönlichkeit für die Kontrollstelle (wie in Slowenien und in Spanien) oder etwa die Kodifizierung ihrer Befugnisse und ihres Aufgabenbereichs in der Verfassung positive Beispiele für die formelle Verbesserung der Unabhängigkeit von Kontrollstellen darstellen. Auch wenn ihre Wahl durch die Legislative nicht notwendigerweise die Unabhängigkeit der Mitarbeiter der Kontrollstelle gewährleistet, sollten Verfahren, die einen Konsens zwischen Mehrheit und Opposition erfordern, als vielversprechende Praktik betrachtet werden. Ein weiteres Mittel, das eine gegen aussen bekräftigte Unabhängigkeit der Datenschutzbehörde anzeigt, ist in Slowenien vorgesehen, wo die nationale Datenschutzbehörde eine Klagebefugnis besitzt, um die Verfassungsmässigkeit von Rechtsvorschriften durch das Verfassungsgericht prüfen lassen zu können.

Auch die Befugnis der Datenschutzbehörden, sich aktiv an der Ausarbeitung und Vorlage von Verhaltenskodex zu beteiligen, ist u. E. als positives Verfahren zu bewerten. Die Unterstützung bei der Ausarbeitung von Verhaltenskodexes in Datenschutzfragen bzw. deren alleinige Ausarbeitung kommt nämlich nicht nur dem allgemeinen Schutz der Bürger zugute, sondern trägt auch zur Steigerung der Sichtbarkeit der nationalen Datenschutzbehörden in der Gesellschaft bei.

Auf **funktionaler Ebene** sehen sich mehrere Datenschutzbehörden mit einem Mangel an personellen und angemessenen finanziellen Ressourcen konfrontiert (z.B. Frankreich, Italien, Finnland oder Niederlande). In mehreren untersuchten Staaten sind die Datenschutzbehörden laut den in der Literatur geäusserten Auffassungen[305] aufgrund der begrenzten Mittel und nicht in der Lage, ihre Aufgaben vollständig auszuführen. Für die Kontrollstellen sind jedoch finanzielle Unabhängigkeit und Fachkräfte nicht nur unverzichtbar, um einen wirksamen Schutz des Rechts auf Datenschutz zu

[305] Vgl. dazu Datenschutz in der die Rolle der nationalen Datenschutzbehörden Stärkung der Grundrechte-Architektur in der EU – Teil II; http://fra.europa.eu/sites/default/files/tk3109265dec_de_web.pdf, S. 44

gewährleisten, sondern stellen auch eine Voraussetzung für eine echte Unabhängigkeit vom Willen der Regierung dar. Eine direkte Kontrolle der finanziellen Mittel und eine selbständige Kompetenz zur Einstellung der Fachkräften können eine solche Unabhängigkeit gewährleisten. Dies ist z.B. in Slowenien vorgesehen.

Auf **operativer Ebene** wiederum sind die Befugnisse eine Voraussetzung für die Wirksamkeit der Datenschutzregelungen. Hier könnten nach unserer Auffassung die begrenzten Befugnisse mehrerer Kontrollstellen ein Problem darstellen (z.B. Deutschland, Vereinigtes Königreich, Frankreich), insbesondere wenn die Behörde keine Untersuchungs- oder Einwirkungsbefugnisse (Verbote, etc.) hat.

Die Datenschutzbehörden müssen über die erforderlichen Ressourcen und Befugnisse verfügen und die nötige Unabhängigkeit besitzen, um zur wirksamen Durchsetzung des Datenschutzsystems beitragen zu können. Garantien für eine wirksame Durchsetzung des Datenschutzes sowie für effiziente Untersuchungen und die zuverlässige Erkennung von Zuwiderhandlungen sind entscheidend, um Verstösse gegen den Datenschutz zu unterbinden. Eine nachdrückliche Durchsetzung würde auch dazu beitragen, die Betroffenen davon zu überzeugen, dass datenschutzrechtliche Bedenken ernst genommen werden. Die Datenschutzbehörden sollten eine wichtige Rolle bei der Durchsetzung des Datenschutzsystems spielen; dazu sollte ihnen entweder die Befugnis zur unmittelbaren Verhängung von Sanktionen oder die Befugnis zur Einleitung von Verfahren übertragen werden, in denen Sanktionen von Amts wegen verhängt werden können.

Als Beispiel eines guten Ansatzes in oben erwähnten Hinsichten könnten die verhältnismässig neuen Regelungen in Polen und Slowenien dienen, wobei in der Praxis hier noch relativ wenige Erfahrungen vorhanden sind.

SCHWEIZERISCHES INSTITUT FÜR RECHTSVERGLEICHUNG

Dr. Lukas Heckendorn Urscheler
Leiter der wissenschaftlichen Abteilung

Dr. Josef Skala
Projektleiter, wissenschaftlicher Mitarbeiter