

FRA

Thematic Legal Study on assessment of
data protection measures and relevant
institutions
Belgium

Leuven, Belgium
March 2009

Paul Lemmens (co-ordinator)
Pierre Schmitt

DISCLAIMER: This thematic legal study was commissioned as background material for the comparative report on *Data protection in the European Union: the role of National Data Protection Authorities* by the European Union Agency for Fundamental Rights (FRA). It was prepared under contract by the FRA's research network FRALEX. The views expressed in this thematic legal study do not necessarily reflect the views or the official position of the FRA. This study is made publicly available for information purposes only and do not constitute legal advice or legal opinion.

Contents

Executive summary	3
1. Overview.....	7
1.1. Overview of constitutional and international standards relevant for data protection in Belgium.....	7
1.1.1. Constitutional standards.....	7
1.1.2. International standards.....	7
1.2. Overview of national data protection legislation	8
2. Data Protection Authority	11
2.1. Presentation	11
2.2. Powers of the data protection authority	13
2.3. Remit of the data protection authority	15
2.4. Resources.....	16
2.5. Independence.....	16
2.6. Right of initiative of the CPPL.....	17
2.7. Monitoring role of the CPPL	18
2.8. Publication of the opinions and recommendations of the CPPL ..	19
2.9. Binding force of opinions of the Working Party established under Article 29 of Directive 95/46/EC.....	20
2.10. Advisory role of the CPPL	20
2.11. Awareness raising role of the CPPL.....	21
3. Compliance.....	23
3.1. Registration of data processing operations	23
3.2. Authorisation of sensitive and other data processing operations ..	24
3.3. Appointment of data protection officials	26
3.4. Compliance or lack of compliance with data protection legislation in practice	26
4. Sanctions, Compensation and Legal Consequences	29
4.1. Sanctions and remedies in general.....	29
4.2. Personal initiative of data subjects in the enforcement of data protection legislation	31
4.3. Protection of personal data in the context of employment	32
5. Rights Awareness.....	34
6. Analysis of deficiencies.....	35
6.1. Deficiencies regarding effective data protection	35
6.2. Deficiencies regarding effective institutions	35
6.3. Suggestions to fill or reduce these deficiencies	36
7. Good practices	37
8. Miscellaneous	39
Annexes	41

Executive summary

Overview

- [1]. The processing of personal data is regulated by the federal Act of 8.12.1992 on the protection of private life with respect to processing of personal data (Data Protection Act). This Act defines the rights and duties of the person whose data are processed but also those of the controller of this processing. Moreover, this law sets up an independent control organ, the *Commissie voor de Bescherming van de Persoonlijke Levenssfeer* (CBPL) – *Commission de la Protection de la Vie Privée* (CPVP) [Commission for the Protection of Private Life (hereafter: CPPL)].

Data Protection Authority

- [2]. The CPPL is an independent control body, set up to protect the private life with respect to processing of personal data. The CPPL essentially has four missions. First, it gives opinions and recommendations to public institutions processing personal data and sometimes to private persons who are controllers of such processing. Secondly, it can grant authorisations to organisms to process and communicate certain personal data. In general, however, such authorisations are granted by the sector committees, mentioned below. Thirdly, the CPPL can receive and examine complaints. Fourthly, the CPPL watches over the smooth running of the processing and communication of personal data, and in this respect it informs and assists citizens and controllers of the processing. The CPPL thus contributes to the protection of privacy while maintaining a necessary balance between the various interests involved.

Compliance

- [3]. In accordance with Article 17 of the Data Protection Act, prior to the start of an entirely or partially automated processing of personal data with a given finality or a number of connected finalities, the controller of the processing shall declare it to the CPPL. Moreover, apart from the issue of sensitive data, in the strict sense of the word, mention should also be made of a number of statutory provisions

that, for various reasons, submit the processing or the communication of certain personal data to a prior authorisation.

- [4]. If someone runs into difficulties in trying to exercise his/her rights, or if a controller of the processing does not respect his/her obligations, the data subject may file a complaint with the CPPL. If the complaint is admissible, the CPPL acts as a mediator and tries to bring the parties to a friendly settlement. If no settlement can be reached, the CPPL adopts an opinion. Moreover, it denounces criminal offences to the public prosecutor, and its president can submit to the court of first instance any claim relating to the application of the Data Protection Act and the measures in execution thereof. Of course, the data subject may directly bring a claim before the tribunal or file a complaint with the public prosecutor.

Sanctions, Compensation and Legal Consequences

- [5]. Under the system of the Data Protection Act, the CPPL can find that a particular processing of personal data violates the right to respect for privacy, but it cannot impose any sanction or take any remedial measure. If further action is needed, it is for the courts to take it.
- [6]. As far as criminal proceedings are concerned, the Data Protection Act contains no specific rules. The common criminal procedure will apply.
- [7]. As far as civil proceedings are concerned, Article 14 of the Data Protection Act provides for a special procedure before the president of the court of first instance. That procedure can be used for claims relating to the data subject's right of access and his/her right to obtain the rectification, erasure or blocking of data that are incorrect or the processing of which is not compatible with the Act. In all other cases, the common procedure before the ordinary courts, in particular the court of first instance, will be available.

Rights Awareness

- [8]. In its management plan of 2003, the CPPL mentions that it wants to contribute to a better information of both controllers of processings and data subjects. This may be achieved through responses to requests for information and through an active communication system.

Analysis of deficiencies

- [9]. There are some uncertainties concerning the scope of the Data Protection Act, and notably the concept of 'file'.

Good Practice

- [10]. Specialised sector committees have been created by law within the CPPL, in order to relieve the CPPL from having to overview the processing of personal data in various specific sectors or with respect to specific systems of data processing. These committees are composed in equal shares of members of the CPPL and experts chosen for their practical knowledge in the concerned sector. Currently, six sector committees have been created, namely for the sector of social security and health, for the national register of natural persons, for the federal administration, for the central data bank for undertakings, for the judicial information system 'Phenix' and for the sector of public statistics.
- [11]. After the Court of Cassation had found that the Data Protection Act did not apply to video surveillance, the legislator filled the gap. An Act of 21.03.2007 concretely sets principles similar to those of the Data Protection Act and provides clear rules for control and information.

Miscellaneous

- [12]. Recently, an interesting debate on data protection concerned a federal Act promulgated on 21.08.2008 and organising a platform called 'e-health'. The 'e-Health Platform' is a public institution that will organise an electronic exchange of medical and other data between health care professionals and institutions, in order to simplify and improve the health care system. Some organisations of doctors protested that the privacy of patients was not sufficiently protected, notably because health insurance funds and social security institutions will have access to the platform. Asked to give an opinion on the bill, the CPPL, however, did not raise any major objection.
- [13]. Another important debate is still going on in the Parliament. It concerns the possible creation of a national databank to be held by the police. Initially, the idea was to organise it by royal decree. However, after parliamentarians raised concerns, the Minister of

Justice agreed to have a discussion on the most sensitive issues and to consider the tabling of a bill which would then allow for a parliamentary debate.

1. Overview

1.1. Overview of constitutional and international standards relevant for data protection in Belgium

1.1.1. Constitutional standards

[14]. Article 22, para. 1, of the Belgian Constitution guarantees the right to respect for private and family life, except in the cases and under the conditions provided by law. Article 22, para. 2, provides that federal laws and community and regional decrees shall guarantee the protection of this right.

[15]. At first view, Article 22, para. 1, of the Constitution does not seem to set substantive conditions for restrictions of the right guaranteed by it. However, according to the Constitutional Court, Article 22 has to be interpreted in the light of the international treaty provisions relating to the right to respect for private life and family life, in particular Article 8 of the European Convention on Human Rights and Article 17 of the International Covenant on Civil and Political Rights. This implies, in particular, that the conditions for the lawfulness of an interference with the said right are those that are set out explicitly in the said treaty provisions.¹

1.1.2. International standards

[16]. Within European Union law, Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data constitutes the principal norm in regard

¹ See, e.g., Belgium/Constitutional Court/162/2004 (20.10.2004), available at www.arbitrage.be (24.1.09); Belgium/Constitutional Court/16/2005 (19.01.2005), available at www.arbitrage.be (24.1.09). Both judgments concerned the constitutionality of a decree of the Flemish Community, which contained an obligation for sports associations to publish any disciplinary decision suspending a sportsman for use of prohibited products (doping) on an official website of the Flemish Community. Such publication had to contain the name and the date of birth of the sportsman, the beginning and the end of the suspension period and the relevant sport discipline. The Constitutional Court held that this obligation violated Article 22 of the Constitution, as it imposed a disproportionate burden on the sportsmen.

of processing of personal data.² This directive has been implemented in the Belgian legal order through an Act of 11.12.1998.³

- [17]. The directive builds on the Convention for the Protection of Individuals relating to Automatic Processing of Personal Data, adopted by the Member States of the Council of Europe on 28.01.1981.⁴ It intends to protect the private life of citizens with respect to processing of personal data, but only where such processing takes place by automated means. This convention is by now binding for all Member States of the European Union. It has been ratified by Belgium on 28.05.1993.
- [18]. The Organisation for Economic Co-operation and Development (OECD)'s Council issued on 23.09.1980 a recommendation with guidelines governing the protection of privacy and transborder flows of personal data.⁵ These guidelines are the result of an international consensus on the acceptable practices to be respected by the business sector when collecting and processing personal data.

1.2. Overview of national data protection legislation

- [19]. According to the above mentioned Article 22, para. 1, of the Constitution, it is for the federal legislator to set the minimum conditions for any interference in the right to respect for private life and family life. These minimum norms are binding, not only for the

² Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24.10.1995), *Official Journal of the European Communities*, No. L 281 (23.11.1995), p. 31.

³ Belgium/Wet tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens (11.12.1998), *Moniteur belge* (03.02.1998), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) Dutch; Belgium/Loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (11.12.1998), *Moniteur belge* (03.02.1998), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁴ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28.01.1981), available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (12.01.2009).

⁵ OECD, Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (23.09.1980), available at www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

federal authorities, but also for all authorities, including the legislative authorities, of the communities and the regions.⁶

- [20]. With respect to the processing of personal data, the general norms, acting as minimum norms, are set by the federal Act of 8.12.1992 on the protection of private life with respect to processing of personal data, hereafter the Data Protection Act.⁷ This Act defines the rights and duties of the person whose data are processed but also those of the controller of this processing. Moreover, this law sets up an independent control organ, the *Commissie voor de Bescherming van de Persoonlijke Levenssfeer* (CBPL) – *Commission de la Protection de la Vie Privée* (CPVP) [Commission for the Protection of Private Life (hereafter: CPPL)]. Since its promulgation, the Data Protection Act has been subject to important amendments. The first one is a consequence of the adoption of the above mentioned Directive 95/46/EC⁸, which has been transposed into the Belgian legal order through the already mentioned Act of 11.12.1998.⁹ Another important modification has been initiated by the Belgian legislator in order to respond to the rapid evolution of the information society. The CPPL was increasingly requested to deliver opinions on sharp questions which required very specific expertise. As a consequence, the Act of 26.02.2003¹⁰ has modified the status, the composition and

⁶ See, e.g., Belgium/Constitutional Court/162/2004 (20.10.2004), available at www.arbitrage.be (24.1.09); Belgium/Constitutional Court/16/2005 (19.01.2005), available at www.arbitrage.be (24.1.09).

⁷ Belgium/Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁸ Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24.10.1995), *Official Journal of the European Communities*, No. L 281 (23.11.1995), p. 31.

⁹ Belgium/Wet tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens (11.12.1998), *Moniteur belge* (03.02.1998), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) Dutch; Belgium/Loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (11.12.1998), *Moniteur belge* (03.02.1998), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

¹⁰ Belgium/Wet tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation

the competences of the CPPL and created various specialised committees. One of the changes brought by this Act is that it elevated the CPPL from an organ dependent on the Minister of Justice to an organ directly linked to the House of Representatives.

d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

2. Data Protection Authority

2.1. Presentation

- [21]. The CPPL is an independent control body, set up to protect the right to private life with respect to the processing of personal data.¹¹ It was established in 1992 by the Data Protection Act.¹² The CPPL is composed of 16 members: a president, a vice-president, six other effective members and eight substitute members. Both the president and the vice-president exercise their function on a full time basis. The mandate of president is reserved to a magistrate. The mother tongue of the vice-president has to differ from the president's one. The CPPL has to comprise at least one other lawyer, a computer scientist and two persons having professional experience in the domain of management of personal data, respectively in the public and the private sector. The 16 members are designed for a period of six years. Their mandate is renewable.
- [22]. The CPPL essentially has four missions. First, it gives opinions and recommendations to public institutions processing personal data and sometimes to private persons who are controllers of such processing. Secondly, it can grant authorisations to organisms to process and communicate certain personal data. In general, however, such authorisations are granted by the sector committees, mentioned below.¹³ Thirdly, the CPPL can receive and examine complaints. Fourthly, the CPPL watches over the smooth running of the processing and communication of personal data, and in this respect it informs and assists citizens and controllers of the processing. The CPPL thus contributes to the protection of privacy while maintaining a necessary balance between the various interests involved.
- [23]. Specialised sector committees have been created by law within the CPPL, in order to relieve the CPPL from having to overview the

¹¹ The name of the CPPL is somewhat misleading. It has no competence with respect to private life generally, but only with respect to private life insofar as it is affected by the processing of personal data.

¹² Belgium/Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

¹³ See no. [23].

processing of personal data in various specific sectors or with respect to specific systems of data processing. According to Article 31bis § 2 of the Data Protection Act, these committees are composed in equal shares of members of the CPPL and experts chosen for their practical knowledge in the concerned sector. Currently, six sector committees have been created, namely for the sector of social security and health¹⁴, for the national register of natural persons¹⁵, for the federal administration¹⁶, for the central data bank for undertakings¹⁷, for the judicial information system 'Phenix'¹⁸ and for the sector of public statistics.¹⁹ For each committee there is a separate statutory basis. The experts of the committee for the sector of public statistics have not been appointed thus far and that committee's competences are actually still exercised by the CPPL itself.

-
- ¹⁴ Belgium/Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (15.01.1990), *Moniteur belge* (22.02.1990; errata, *Moniteur belge* (02.06.1990) & *Moniteur belge* (02.10.1990)), available at www.ejustice.just.fgov.be/wet/wet.htm, consolidated version (29.03.2007) available at www.privacycommission.be/nl/static/pdf/wetgeving/wet_kruispuntbank_sociale_zekerheid.pdf (24.01.1999) (Dutch); Belgium/Loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (15.01.1990), *Moniteur belge* (22.02.1990; errata, *Moniteur belge* (02.06.1990) & *Moniteur belge* (02.10.1990)), available at www.ejustice.just.fgov.be/wet/wet.htm, consolidated version (29.03.2007) available at www.privacycommission.be/fr/static/pdf/wetgeving/loi_banque_carrefour_securite_sociale.pdf (24.01.2009) (French).
- ¹⁵ Belgium/Wet tot regeling van een Rijksregister van de natuurlijke personen (8.08.1983), *Moniteur belge* (21.04.1983), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi organisant un registre national des personnes physiques (8.08.1983), *Moniteur belge* (21.04.1983), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).
- ¹⁶ Belgium/Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).
- ¹⁷ Belgium/Wet tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen (16.01.2003), *Moniteur belge* (05.02.2003), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi portant création d'une Banque-carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions (16.01.2003), *Moniteur belge* (05.02.2003), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).
- ¹⁸ Belgium/Wet tot oprichting van het informatiesysteem Phenix (10.08.2005), *Moniteur belge* (01.09.2005), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi instituant le système d'information Phénix (10.08.2005), *Moniteur belge* (01.09.2005), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).
- ¹⁹ Belgium/Wet betreffende de openbare statistiek (04.07.1962), *Moniteur belge* (20.07.1962), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la statistique publique (04.07.1962), *Moniteur belge* (20.07.1962), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

- [24]. The CPPL carries out its tasks with a secretariat, composed of fifty-four agents.

2.2. Powers of the data protection authority

- [25]. Article 28 (2-4) of Directive 95/46/EC sets up a list of requirements to be met by the Member States with respect to the data protection authority, in order to ensure effective data protection. The Belgian CPPL seems to comply with these requirements.
- [26]. First of all, Article 28 (2) of the Directive requires that the data protection authority has to be consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. In Belgium, Articles 29 and 30 of the Data Protection Act provide that the CPPL issues either at its own initiative or at the request of a federal, community or regional government or parliamentary assembly or a sector committee, opinions and recommendations on every question relating to the application of fundamental principles of protection of privacy in the framework of the Data Protection Act or any other law containing provisions on privacy regarding the processing of personal data.
- [27]. Article 28 (3) of the Directive provides that the data protection authority should be endowed with investigative powers, effective powers of intervention and the power to engage in legal proceedings where the national provisions adopted pursuant to the Directive have been violated or to bring these violations to the attention of the judicial authorities.
- [28]. As far as the investigative powers are concerned, those of the CPPL are described primarily in Article 32 § 1 of the Data Protection Act. Its rules of internal order contain further specifications with respect to controls (of an individual controller of a processing) and inspections (of a group of controllers or even an entire sector). The CPPL can request the assistance of experts for the accomplishment of its missions. It may charge one or several of its members with an investigation on the spot. In such a case, the members of the CPPL have the same powers as a police officer engaged in a judicial investigation. They may notably require the communication of any document which could be useful to their investigation. They may also enter into any places for which they have a reasonable ground to presume that an activity in relation to the Data Protection Act is carried out. According to Article 40 of the CPPL's rules of internal

order, the investigation has to be described in a report.²⁰ The controller of the processing is informed of the aim of the investigation and of the applicable law. A copy of the report is immediately transmitted and the controller may write a declaration or a commentary and/or ask it to be attached to the report.

- [29]. As far as the effective powers of intervention are concerned, the Directive contains an illustrative list of possible powers: ‘that of delivering opinions before processing operations are carried out, [...] and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions’. The Belgian Data Protection Act does not follow these examples: the CPPL in general does not give an opinion prior to the start of processing operations, it cannot order the blocking, erasure or destruction of data, nor can it impose a temporary or definitive ban on processing, nor can it refer a matter to a political institution. The only power that comes close to one that is mentioned in the Directive is that of making a recommendation to the controller. This does not mean that the Belgian law does not comply with the Directive on this point. As the list does not have a normative character, the Belgian legislator could consider that the effectiveness of the CPPL’s power of intervention was assured by other means.
- [30]. As far as the power to engage in legal proceedings or to bring violations to the attention of the judicial authorities is concerned, Article 32 § 2 of the Data Protection Act provides that the CPPL can denounce criminal offences to the public prosecutor. This possibility is an important ‘stick behind the door’. Moreover, according to Article 32 § 3 of the Act, notwithstanding the general competence of ordinary courts, the president of the CPPL may submit to the court of first instance any claim concerning the application of the Data Protection Act and the measures in execution thereof.
- [31]. Article 28 (4) of the Directive provides that each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. In

²⁰ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Huishoudelijk reglement, available at www.privacycommission.be/nl/static/pdf/cbpl-documents/huishoudelijk-reglement.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, Règlement d’ordre intérieur, available at www.privacycommission.be/fr/static/pdf/r-glement_ordre-int-rieur.pdf (24.01.2009) (French).

Belgium, the CPPL may receive complaints from every person justifying an interest.²¹ Article 31 § 1 of the Data Protection Act provides that the CPPL examines every complaint addressed to it in relation to the CPPL's mission concerning the protection of private life with respect to the processing of personal data or concerning any other mission conferred to the CPPL by law. The procedure is governed by the rules of internal order. In conformity with the principle enunciated in Article 31 § 2 of the Data Protection Act, these rules provide for an adversarial procedure. The main steps in the procedure are set out in Article 31 § 3 of the Act. The CPPL first takes a decision on the admissibility of the complaint. If the complaint is admissible, the CPPL will accomplish every mission of mediation it deems useful. Indeed, the CPPL shall in all circumstances act in such a way as to promote a friendly settlement between the complainant and the controller of the processing.²² In case a settlement between the parties is reached, based on respect of privacy, the CPPL drafts a report in which it includes the terms of the agreement. If no settlement is reached, the CPPL adopts an opinion on the merits of the complaint. It can add recommendations to its findings, at the attention of the controller. According to Article 31 § 4 of the Data Protection Act, every decision (on admissibility), opinion (on the merits) and recommendation adopted by the CPPL has to be motivated. Article 31 § 5 finally provides that the decision, opinion or recommendation is communicated to the complainant, to the controller and to every other party in the proceedings. A copy of the decision, opinion, and recommendation is also communicated to the Minister of Justice.

2.3. Remit of the data protection authority

- [32]. According to Article 3 § 1 of the Data Protection Act, the Act applies to any entirely or partially automated processing of personal data, as well as to any non-automated processing of personal data that are placed in a file or that are intended to being placed therein. The Act applies to any processor, whether he is a natural person, a legal person, an association without legal personality or a public authority (Article 1 § 4). A general exception is made, however, for processings by a natural person for purely personal or domestic

²¹ Art. 25 of the rules of internal order. See Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Huishoudelijk reglement, available at www.privacycommission.be/nl/static/pdf/cbpl-documents/huishoudelijk-reglement.pdf (12.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, Règlement d'ordre intérieur, available at www.privacycommission.be/fr/static/pdf/r-glement_ordre-int-rieur.pdf (12.01.2009) (French).

²² Article 27 of the rules of internal order.

purposes (Article 3 § 2). This scope of application determines in principle also the remit of the CPPL.

- [33]. Moreover, some categories of processing of personal data are specifically excluded from the scope of application of a number of provisions of the Act, and thus also, to that extent, from the remit of the CPPL. This is in particular the case for processing of personal data by police and security services (Article 3 §§ 4 and 5) and by the organisation “Child Focus” (European Centre for Missing and Sexually Exploited Children) (Article 3 §§ 6 and 7).

2.4. Resources

- [34]. In accordance with Article 34 of the Data Protection Act, the CPPL submits its annual budget to the House of Representatives for approval. The proposed budget is accompanied by a management plan. The annual activity report shall describe the follow up reserved to the plan.
- [35]. Since 01.12.2004, the CPPL has proper budgetary means at its disposal, as an auxiliary organ of the House of Representatives. For 2008, the budget of the CPPL was fixed at 5,340,000 €. ²³ This budget includes the full time members’ salaries, the attendance fees for the other members, the salaries of the personnel in the secretariat and all the other costs of operation.
- [36]. As indicated above, the House of Representatives has fixed the number of staff members in the secretariat at fifty-four. A problem encountered by the CPPL, as long as it was under the administrative authority of the Ministry of Justice, was the lack of staff members staying for a sufficiently long time with the CPPL. The CPPL management plan of 2003 announced measures to improve the organisation of the staff, in order to make sure that the CPPL has specialists at its disposal, develops expertise and increases flexibility in human resources management.

2.5. Independence

- [37]. Article 24 § 6 of the Data Protection Act states that within the limits of their attributions, the president and the members of the CPPL

²³ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Middelen*, available at www.privacycommission.be/nl/commission/about/means (12.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Moyens*, available at www.privacycommission.be/fr/commission/about/means (12.01.2009) (French).

may not receive instructions of anybody. They may not be relieved of their duties by reason of their opinions issued or acts accomplished to fulfil their function. Article 24 § 4 furthermore states that members have to offer all guarantees for an independent exercise of their mission and that they have to be fully competent in the domain of protection of data. In practice, the CPPL has always enjoyed an effective independence as far as the substance of its activities is concerned.

- [38]. Another issue is whether the CPPL disposes of the practical means to fulfil its mandate. Before the Act of 26.02.2003²⁴ the CPPL was an organ administratively dependent on the Minister of Justice. This dependence created some difficulties. Indeed, one could notice a constant reduction of its staff – its secretariat was reduced from 34 full-time equivalents in 1997 to 18,5 in 2003. Moreover, many staff members left after a relatively short time, notably because of the discrepancy between the required level of competence and the career possibilities, and because of the fact that public institutions, specialised law firms and private undertakings proposed to the agents some more interesting functions and salaries than those offered by the CPPL. In order to acquire a greater autonomy, the CPPL in 2001 informed the Parliament of its wish to be attached to it. Parliament reacted favourably to that request. The Act of 26.02.2003 has elevated the CPPL from an organ dependent on the Minister of Justice to an organ directly linked to the House of Representatives, thus increasing its organisational and budgetary autonomy.²⁵

2.6. Right of initiative of the CPPL

- [39]. According to Articles 29 and 30 of the Data Protection Act, the CPPL may issue opinions and recommendations at its own initiative

²⁴ Belgium/Wet tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

²⁵ Belgium/Senate, Bill tabled by Mr Roelants du Vivier, *Documents parlementaires*, extraord. session 2003, no. 3-40/1 (08.07.2003), p. 4 available at http://www.senate.be/www/?Mival=/index_senate&MENUID=22101&LANG=nl (15.03.2009).

on every question relating to the application of the fundamental principles of protection of privacy in the framework of the Data Protection Act or of any other law containing provisions on privacy regarding processing of personal data. As explained above, the CPPL also has control and inspection competences, which it can exercise at its own initiative. As was noted in the above mentioned management plan, until 2003, due to a lack of means, both control and inspection were undertaken only on the basis of a complaint. The management plan sets a number of objectives in order to improve the control and inspection system.²⁶ In its annual activity report of 2007, the CPPL noted that most controls had by then been executed by the CPPL at its own initiative. In 66 per cent of the cases, the controls and inspections were generally focused on one particular sector.²⁷ In 2007, three sectors in particular received attention, namely those of the energy suppliers, the financial institutions and the digital television suppliers.

2.7. Monitoring role of the CPPL

- [40]. If the CPPL wants to fulfil its monitoring mission, it has to perform efficient controls and inspections, with authority and in a realistic lapse of time. In its management plan of 2003 the CPPL noted that this mission was at that time in an embryonic status, as the CPPL had to give priority to requests from outside the CPPL. Both inspection and control had only been undertaken on the basis of complaints, not at the initiative of the CPPL itself, due to lack of means. The CPPL was aware of the fact that it had to give a particular attention to the monitoring activity in order to acquire the confidence of citizens in the information society. If it wanted to remain credible and concretise its vision, it also had to fix for itself clear deadlines. The management plan therefore set concrete objectives, in order to reinforce the monitoring role of the CPPL.²⁸

²⁶ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at

www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (24.01.2009) (French).

²⁷ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Jaarverslag 2007*, available at www.privacycommission.be/nl/static/pdf/annual-reports/jaarverslag-2007.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Rapport annuel 2007*, available at www.privacycommission.be/fr/static/pdf/annual-reports/rapport-annuel-2007.pdf (24.01.2009) (French).

²⁸ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (24.01.2009) (French).

These objectives were: the elaboration of an organisational schema with a particular concern for the simplification of procedures; concern for the mediation function; concern for the safety of the processing, and the contribution to an innovative thinking in this matter; the introduction of project management with the possibility to create multidisciplinary teams; the setting-up of a control system of quality; the creation of a follow-up system. The management plan also recommended the recruitment of additional lawyers and assistants in order to improve the monitoring role of the CPPL.

2.8. Publication of the opinions and recommendations of the CPPL

- [41]. The CPPL communicates its opinions to the requesting authority and sends a copy of them to the Minister of Justice. If the opinion is on a draft regulation and the consultation of the CPPL is required by law, the opinion has to be published in the official gazette (*Moniteur belge*), together with the regulatory act to which it relates. Concerning recommendations to a controller of a processing, the CPPL sends a copy to the Minister of Justice. In case of a complaint, the Commission communicates its decision, opinion or recommendation to the plaintiff, to the controller and to all parties in the proceedings. A copy of the decision, opinion or recommendation is sent to the Minister of Justice.
- [42]. Article 14 of the CPPL's rules of internal order provides for the possibility for the CPPL to give another form of publicity to its opinions, recommendations and decisions, in addition to the publicity imposed by law.²⁹ Opinions and recommendations are normally published on the website of the CPPL, unless the CPPL decides otherwise, in a motivated decision. The authority requesting an opinion may ask that the opinion will not be made public. The CPPL must accede to such demand, unless it considers that the non-publication is incompatible with the principles of a democratic state governed by the rule of law and with human rights. It then motivates the refusal and publishes it as an attachment to its opinion. The rules of internal order provide that the CPPL develops a website on which all its decisions, except for those that belong to the exceptions

²⁹ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Huishoudelijk reglement, available at www.privacycommission.be/nl/static/pdf/cbpl-documents/huishoudelijk-reglement.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, Règlement d'ordre intérieur, available at www.privacycommission.be/fr/static/pdf/r-glement_ordre-int-rieur.pdf (24.01.2009) (French).

indicated above, are made public. The public register and the system of declarations are also accessible through the website.

2.9. Binding force of opinions of the Working Party established under Article 29 of Directive 95/46/EC

- [43]. The opinions of the Working Party established under Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are considered as an important source of inspiration for the interpretation by the CPPL of national legislation implementing the EU legislation on data protection. Indeed, the CPPL frequently refers to the explanations or definitions agreed upon within the Working Party. For instance, the CPPL issued on 15.06.2005 an opinion concerning the framing of black lists³⁰ in which the definition of ‘black list’ refers to working document no. 65 on black lists adopted by the Working Party on 3.10.2002.³¹

2.10. Advisory role of the CPPL

- [44]. The CPPL can issue opinions and recommendations on the processing of personal data in accordance with Articles 29 and 30 of the Data Protection Act. Most frequently, the CPPL intervenes upon a request by the authority concerned or by a sector committee, but it may also decide on its own initiative to formulate an opinion or a recommendation. An opinion on a complaint or a decision on the declaration of a processing may also include a recommendation to

³⁰ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 09/2005 (15.06.2005), available at www.privacycommission.be/nl/docs/Commission/2005/advies_09_2005.pdf (12.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, Avis no. 09/2005 (15.06.2005), available at www.privacycommission.be/fr/docs/Commission/2005/avis_09_2005.pdf (12.01.2009) (French).

³¹ According to the Working Party’s working document no. 65 on black lists, 11118/02/EN/final (03.10.2002), available at http://europa.eu.int/comm/justice_home/fs/privacy/studies/index_en.htm (24.01.2009), ‘a blacklist could be said to consist of the collection and dissemination of specific information relating to a specific group of persons, which is compiled to specific criteria according to the kind of blacklist in question, which generally implies adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.’

the controller of the processing. With respect to opinions and recommendations, the CPPL's management plan of 2003 foresees some measures to increase its performance in order to obtain immediate results and to contribute in an innovative way, via the opinions and recommendations, to the definition of data protection standards, both at national and international level.³² This approach requires solid work of high quality, a proactive management of knowledge, a management of time, and techniques of follow-up. In order to increase the quality and the effectiveness of its work, the CCPL has decided to entrust its staff with the preparation of opinions and recommendations, so that the members of the CPPL can concentrate on the substantive aspects and on the policy issues.

- [45]. As indicated above, since the amending Act of 26.02.2003 the CPPL is an auxiliary organ of the House of Representatives.³³ The CPPL received this status having regard, among other things, to its mission of control of the executive. The expectation was that the new status should incite Parliament to ask the CPPL more frequently for its opinion on draft legislation.³⁴ In practice the CPPL is indeed regularly consulted, especially where sensitive issues arise.

2.11. Awareness raising role of the CPPL

- [46]. In its management plan of 2003, the CPPL mentioned that it wanted to contribute to a better information of public.³⁵ This would be achieved through responses to information demands and through the

³² Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (24.01.2009) (French).

³³ Belgium/Wet tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée (26.02.2003), *Moniteur belge* (26.06.2003), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

³⁴ Belgium/House of Representatives, *Documents parlementaires*, 2001-02, no. 50-1940/5, p. 4.

³⁵ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/ Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (12.01.2009) (French).

development of an active communication system, relying notably on a renovated website and on explanation notes addressed to public. At a later stage a publicity campaign would be launched.

- [47]. The last annual report (2007) echoes these objectives. The CPPL recognises that it has to raise the awareness of citizens for their rights and to inform them of the main issues relating to privacy and data protection. In addition, private and public actors working on the personal data processing have to be attentive to legal principles, to be aware of the fundamental rights of citizens, to respect these rights and to take concrete measures aiming at guaranteeing the security of information and the protection of privacy.³⁶

³⁶ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Jaarverslag 2007*, available at www.privacycommission.be/nl/static/pdf/annual-reports/jaarverslag-2007.pdf (12.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Rapport annuel 2007*, available at www.privacycommission.be/fr/static/pdf/annual-reports/rapport-annuel-2007.pdf (12.01.2009) (French).

Compliance

2.12. Registration of data processing operations

- [48]. In accordance with Article 17 of the Data Protection Act, prior to the start of an entirely or partially automated processing of personal data with a given finality or a number of connected finalities, the controller of the processing shall declare it to the CPPL. This declaration allows the CPPL to control the compatibility of the declared processing with the law. The declaration is also important because it obliges the controller to state the purposes for which the data will be processed.
- [49]. The automated processing of data may be declared to the CPPL through two channels: either the controller completes a form directly on the CPPL website, or he prints the form and fills it out. A contribution is due for each declaration: 25 € if the declaration is electronically introduced, 125 € if the paper form is used. A declaration is also necessary when an existing processing is modified or terminated. Such declaration is subject to the payment of a contribution of 20 €. Article 17 provides a number of elements to be mentioned in the declaration, in particular its date, where applicable the legal basis permitting the creation of the automated processing, the name of the controller of the processing, the name of the automated processing, its finality or the connected finalities, the categories of data processed, the categories of addressees to whom the data may be furnished, the guarantees relating to the communication to third parties, the means by which the data subjects will be informed of the existence of the data processing and the place where they can exercise their right of access, and the period after which the data may not be kept, used or diffused. The CPPL issues a receipt within a delay of three days and transmits the personal identification number, the processing identification number, a copy of the declaration and a bill within 21 days.
- [50]. Certain processings do not fall under this obligation to declare. In the first place, non-automated processings are principally excluded, as for instance paper files. However, manual files can also be concerned, when they constitute a 'structured whole of personal data

accessible following certain criteria'.³⁷ Secondly, certain automated processings are also exempted from the obligation to declare, among which those necessary for the missions of certain authorities (e.g. the secret service of the State) and those the aim of which is only to keep a register which, by virtue of the law, is intended for the information of the general public and is available for public consultation. Thirdly, a number of common processings are also exempted; these exemptions, all based on the idea that there is manifestly no risk for violations of the fundamental rights of the data subjects, are listed in Articles 51-62 of the royal decree of 13.02.2001 executing the Data Protection Act.³⁸ They concern notably the administration of salaries, the administration of staff, accounting and bookkeeping, etc. It should be noted that because of these exemptions, most of the processings are in fact not subject to the obligation of declaring them to the CPPL.

- [51]. According to Article 39 of the Data Protection Act, an infringement of the obligation contained in Article 17 exposes the controller of the processing to a criminal sanction. Indeed, the said article 39, 7° provides that the controller who sets up, manages or terminates an automated data processing without satisfying the requirements set by Article 17 shall be punished with a fine between 100 € and 100,000 €. The same sanction is provided by Article 39, 8° in case of incomplete or inexact information contained in the declaration. In accordance with Articles 40 and 41, the criminal court can impose the publication of its judgment in one or more newspapers, can order the confiscation of material supports of personal data and the erasure of these data, and can prohibit the controller to manage any processing of personal data for a period of up to two years.

2.13. Authorisation of sensitive and other data processing operations

- [52]. The protection of sensitive data is the object of Articles 6 to 8 of the Data Protection Act. Article 6 § 1 provides that the processing of

³⁷ See the definition of 'file' in Article 1 § 3 of the Data Protection Act. See also Court of Appeal of Liège (06.02.2006), *Jurisprudence de Liège, Mons et Bruxelles*, 2006, pp. 665-667; Th. LEONARD & Y. POULLET, 'La protection des données à caractère personnel en pleine (r)évolution', *Journal des Tribunaux*, 1999, p. 371.

³⁸ Belgium/Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (13.02.2001), *Moniteur belge* (13.03.2001), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (13.02.2001), *Moniteur belge* (13.03.2001), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

personal data revealing racial or ethnic origin, political opinions, religious or philosophical convictions or the membership of a trade union, as well as the processing of personal data relating to sex life, are in principle prohibited. Article 6 § 2 provides for a number of exceptions to this general prohibition. One of these exceptions depends on an explicit authorisation granted by the King upon the advice of the CPPL; this is the case for the processing of data by human rights organisations (Article 6 § 2, first paragraph, k). Moreover, Article 6 § 3 provides that organisations for the reintegration of sexual offenders can be authorised by the King, upon the advice of the CPPL, to process sexual data. Article 7 § 1 furthermore provides that the processing of personal data concerning health is in principle prohibited. Article 7 § 2 provides for a number of exceptions to this general prohibition, but in none of these cases is there a requirement of a prior authorisation. Finally, Article 8 § 1 provides that the processing of personal data relating to disputes submitted to ordinary or administrative courts, to suspicions, prosecutions or convictions with respect to criminal offences, or to administrative sanctions or security measures, is in principle prohibited. Article 8 § 2 provides for a number of exceptions to this general prohibition, but again, in none of these cases is there a requirement of a prior authorisation.

- [53]. Apart from the issue of sensitive data, in the strict sense of the word, mention should also be made of a number of statutory provisions that, for various reasons, submit the processing or the communication of certain personal data to a prior authorisation. One example, which has given rise to hundreds of applications, is the obligation for public authorities and private organisations to obtain the authorisation to have access to the national register of natural persons or to make use of the national identification number (attributed by the national register). This requirement and most of the other authorisation requirements relate to a specific sector or a specific processing system. In order to relieve the CPPL of its duty to look into these often technical issues, the legislator has set up sector committees, as indicated above. At this moment, there are six such committees.³⁹ Where there is a competent committee, it is in principle for that committee to grant the authorisation, but the CPPL may always decide to look itself into the matter. There are no indications that the requirements of prior authorisation, where applicable, are not met in practice.

³⁹ See above, no. [23].

2.14. Appointment of data protection officials

[54]. Article 17bis of the Data Protection Act provides that the King, upon the advice of the CPPL, shall identify the processings that contain specific risks for the rights and freedoms of the data subjects, and set specific conditions aimed at protecting the rights and freedoms with respect to these processings. The King can, in particular, order that the controller of the processing has to appoint a person responsible for the data protection, who will then have to assure compliance with the Act and the regulations adopted in execution thereof, in an independent way. In implementing Article 17bis, the King has not made use of the possibility to impose on controllers the obligation to appoint a data protection official. In the explanatory statement relating to the royal decree of 13.02.2001 executing the Data Protection Act, the government explicitly states that the idea of appointing such a person, which stems from Directive 95/46/EC⁴⁰ and from the practice in Germany, did never receive support in Belgium. The government prefers to protect sensitive data by other means, as explained above.⁴¹ If, in the future, there appears to be a need to provide for the appointment of a data protection official, this will have to be the object of a specific decree.⁴²

2.15. Compliance or lack of compliance with data protection legislation in practice

[55]. If someone runs into difficulties in trying to exercise his/her rights, or if a controller of the processing does not respect his/her obligations, the data subject may file a complaint with the CPPL. If the complaint is admissible, the CPPL acts as a mediator and tries to

⁴⁰ Article 18 (2) of Directive 95/46/EC (24.10.1995) states that Member States may, under certain conditions, provide for the simplification of or exemption from notification. One possible and acceptable condition is that 'the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular [...] for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive'.

⁴¹ See no. [52].

⁴² Belgium/Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (13.02.2001), with 'report to the King', *Moniteur belge* (13.03.2001), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (13.02.2001), with 'report to the King', *Moniteur belge* (13.03.2001), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

bring the parties to a friendly settlement. If no settlement can be reached, the CPPL adopts an opinion. Moreover, it denounces criminal offences to the public prosecutor, and its president can submit to the court of first instance any claim relating to the application of the Data Protection Act and the measures in execution thereof.⁴³ The CPPL thus appears to be the body that is primarily responsible for the supervision of compliance with the Data Protection Act. Of course, the data subject may directly bring a claim before the tribunal or file a complaint with the public prosecutor.

- [56]. Some cases that have reached the courts may be mentioned here, by way of example. They illustrate the control exercised by the presidents of the courts of first instance.
- [57]. A data subject may file a claim with the president of the court of first instance, notably in order to obtain an order to rectify or erase data or prohibiting the use of inexact personal data. On 22.03.1994, the President of the Court of First Instance of Brussels had to decide on the lawfulness of the registration of a person in a file of debtors in default of payment. The president held that the general Data Protection Act applied to any processing of data, regardless of whether more specific data protection rules applied in the sector concerned. She further stated that the controller of the processing had to proceed very carefully and to keep the finality of the processing in mind. In this case the controller, a debtor assessment company, had acted unlawfully, as it had simply registered the information furnished by a third party, in this case a bank that had a dispute with the data subject, without controlling whether it was not premature to consider that the data subject did not pay a debt that was due. Turning to the reparation of the damage suffered, the president awarded financial compensation for the non-pecuniary damage and ordered the company to erase the data and, more importantly, to inform its clients of the erasure within five days.⁴⁴
- [58]. On 15.11.1994 the President of the Court of First Instance of Nivelles also was confronted with a claim to order the suppression of data in a file of debtors in default of payment. The president considered that the applicability of the Data Protection Act was not limited because of the fact that the personal data in question presented some commercial or professional aspects. Rules of internal order of a company, which governed the relations between the controller of the processing and the members of the company,

⁴³ See above, no. [30].

⁴⁴ Belgium/President of the Court of First Instance of Brussels (22.03.1994), *Rechtskundig Weekblad*, 1994-95, col. 477, and *Journal des Tribunaux*, 1994, p. 841, with comments Th. LÉONARD.

could not relieve the controller of any liability with respect to persons protected by the Act. The question whether the controller had or had not failed to respect his obligations was therefore to be assessed by the judge. On the merits, the president held that it was not unlawful for the controller, in the light of the concrete circumstances, to consider that the plaintiff had not paid a debt for which she was liable.⁴⁵

- [59]. On 12.04.1995, the President of the Court of First Instance of Brussels had to decide again on the applicability of the Data Protection Act and the scope of the proportionality principle. First of all, he defined personal data as any information concerning a natural person. The general Data Protection Act applied to the processing of such data, regardless of whether the processing took place in a sector for which there were also more special data protection rules. Data appearing in files of a credit assessment company and the National Bank relating to a person's creditworthiness did not fall outside the privacy protection, even if they had also a commercial and professional aspect. Turning to the merits, the president considered that, in order to assess the relevance of data in relation to the finality of the processing, he had a quasi-discretionary power and that he was to be guided by the sole proportionality principle. When the inclusion of a person's personal data in a register is not or no longer proportionate, the president may consider that the use of the data is not relevant and order their erasure. The power conferred upon the president to control the relevance of data in relation to the finality of the processing, would have no sense if the president did not have the possibility, depending on the circumstances of the case, to shorten the delay after which the data had to be erased.⁴⁶

⁴⁵ Belgium/President of the Court of First Instance of Nivelles (15.11.1994), *Journal des Tribunaux*, 1995, p. 284.

⁴⁶ Belgium/President of the Court of First Instance of Brussels/9553 (12.04.1995), summary available at <http://jure.juridat.just.fgov.be> (12.01.2009).

3. Sanctions, Compensation and Legal Consequences

3.1. Sanctions and remedies in general

- [60]. Under the system of the Data Protection Act, the CPPL can find that a particular processing of personal data violates the right to respect for privacy, but it cannot impose any sanction or take any remedial measure. Whether the CPPL acts at its own initiative (inspection and control), or on the basis of a complaint, it can only adopt an opinion on the question of the compatibility with the data protection standards and send a recommendation to the controller. In most cases, however, this appears to be sufficient. In fact, such opinions and recommendations are themselves exceptional, as in most cases a settlement can be reached with the controller. Even more exceptional is the need to take further action, after the finding by the CPPL of an infringement.
- [61]. If further action is needed, it is for the courts to take it. As has been explained above, the CPPL can denounce criminal offences to the public prosecutor, and the president of the CPPL may submit to the court of first instance any claim concerning the application of the Data Protection Act and the measures in execution thereof.⁴⁷
- [62]. Depending on the nature of the alleged shortcoming by the controller of the processing, proof of intent may be required or it may be sufficient to show negligence. Sanctions can be imposed and reparation measures can thus be ordered, even if there has been no intent.
- [63]. As far as criminal proceedings are concerned, the Data Protection Act contains no specific rules. The common criminal procedure will apply.
- [64]. Criminal sanctions are provided by the Data Protection Act for most violations of its provisions. Article 38 states that the controller of the processing who violates the obligations mentioned in Articles 15 and 16 § 1 of the Act, *i.e.* the obligation to mention the existence of a complaint when communicating the disputed data and the obligation of assuring the security of the processing, is punishable

⁴⁷ See above, no. [30].

with a fine from 200 € to 10,000 €. Article 39 enumerates a (long) list of infringements, all punishable with a fine from 100 € to 100,000 €.

- [65]. As far as civil proceedings are concerned, Article 14 of the Data Protection Act provides for a special procedure before the president of the court of first instance.⁴⁸ That procedure can be used for claims relating to the data subject's right of access and his/her right to obtain the rectification, erasure or blocking of data that are incorrect or the processing of which is not compatible with the Act. In all other cases, the common procedure before the ordinary courts, in particular the court of first instance, will be available. The procedure under Article 14 is characterised by its expeditiousness. The president decides on the merits, but the procedure is 'like an interim procedure'.⁴⁹ The procedure is of an adversarial nature, but if serious reasons exist to believe that evidence supporting the claim could be concealed or disappear, the president may *ex parte* order any measure to prevent this concealment or disappearance. The procedure before the president aims to guarantee the respect for the rights granted to data subjects by the Data Protection Act and accordingly makes it possible for the president to call the controller of the processing to order, by imposing or prohibiting certain measures. It is questionable whether the procedure can be used to obtain an award of damages.⁵⁰
- [66]. Two examples taken from the case law can be mentioned.
- [67]. In a case submitted to the President of the Court of First Instance of Brussels, the plaintiff requested the suppression of certain data on the basis of the above mentioned Article 14 of the Data Protection Act. She also claimed damages, arguing that the competence granted by Article 14 was not exclusive and that the president could decide on a connected claim for reparation. The president decided on 19.12.2000 that her competence on the basis of Article 14 was not only exclusive, but also restrictive, in the sense that in an Article 14 procedure she was not able to decide on any other claim than those

⁴⁸ Consult P. LEMMENS (1994) 'De procedure zoals in kort geding betreffende de bescherming van de persoonlijke levenssfeer', in: J. VAN COMPERNOLLE & M. STORME (eds.), *Le développement des procédures "comme en référé". De ontwikkeling van procedures "zoals in kort geding"*, Antwerp-Brussels : Kluwer-Bruylant, p. 175; J.-F. VAN DROOGHENBROECK 'La nature et le régime de la compétence exercée "comme en référé", l'exemple de l'action en dommages et intérêts', *Journal des Tribunaux*, 1996, p. 554; J. HERVEG (2006) 'La procédure "comme en référé" appliquée aux traitements de données', in: J.-F. VAN DROOGHENBROECK (coord.), *Les actions en cessation*, Éditions de la formation permanente Commission Université-Palais (CUP), Brussels: Larcier, p. 220.

⁴⁹ Consult Belgium/President of the Court of First Instance of Brussels (22.03.1994), *Rechtskundig Weekblad*, 1994-95, col. 477, and *Journal des Tribunaux*, 1994, p. 841, with comments Th. LÉONARD.

⁵⁰ Compare the judgment mentioned in note [46], above.

mentioned in Article 14 and notably not on a claim for a remedy, even if such claim was connected to the main claim.⁵¹ This jurisprudence has been confirmed in other cases.⁵²

- [68]. This does of course not mean that reparation is never possible. The Court of Appeal of Liège decided on 05.06.1991, before the enactment of the Data Protection Act, that the processing of a file in the area of consumer credit infringed the rights of personality and protection of the consumer, when the organism exonerated itself of every liability as to the exactness of the data and the use made thereof by its members, deliberately let the debtor in the ignorance of the existence and the content of the file and did not allow him to verify and rectify the data concerning him. The tort liability was consequently established, on the basis of general tort law, and the plaintiff had a right to obtain reparation of the damage suffered.⁵³

3.2. Personal initiative of data subjects in the enforcement of data protection legislation

- [69]. The management plan issued by the CPPL in 2003 noticed that until then, due to lack of means, both inspection and control had only been undertaken by it on the basis of a complaint. As a consequence, the procedure followed was the same as for the examination of a complaint. However, the management plan established a number of objectives in order to improve the system.⁵⁴ In its annual activities report of 2007, the CPPL noticed that most controls executed by the CPPL were at that time launched on the own initiative of the CPPL. In 66 per cent, these controls were generally focused on a given (private) sector.⁵⁵

⁵¹ Belgium/President of the Court of First Instance of Brussels (19.12.2000), *Bulletin des Assurances*, 2001, p. 266, with comments Ch.-A. VAN OLDENEEL.

⁵² See, e.g., Belgium/President of the Court of First Instance of Nivelles (28.10.2003), *Bulletin des Assurances*, 2004, p. 49, with comments Ch.-A. VAN OLDENEEL.

⁵³ Belgium/Court of Appeal of Liège (05.06.1991), *Droit de l'informatique & des télécoms*, 1994, no. 1, p. 32, with comments Th. LÉONARD & E. MONTERO; *Journal des Tribunaux*, 1992, p. 36.

⁵⁴ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/ Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (12.01.2009) (French).

⁵⁵ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Jaarverslag 2007*, available at www.privacycommission.be/nl/static/pdf/annual-reports/jaarverslag-2007.pdf (12.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Rapport annuel*

- [70]. Since the number of cases reported is rather low, it seems that data subjects only rarely resort to the court system for the enforcement of their rights.

3.3. Protection of personal data in the context of employment

- [71]. The labour courts are increasingly confronted with alleged violations by employers of the privacy of their workers. Many of these cases concern the lawfulness of control measures, such as the control of e-mails. Sometimes the Data Protection Act is used as a relevant legal norm. This was the case, *e.g.*, in judgments of 14.12.2004 and 13.09.2005 of the Labour Court of Appeal of Brussels. The court held, among other things, that where an observation led to the identification of individual employees, personal data were processed. Such processing could be justified, but in any event it was necessary that the employees were informed of the fact that their e-mails were subject to inspection. As there was no proof of this in the cases at hand, the court held that the evidence obtained through the control of e-mails was unlawful, and therefore could not be taken into account in assessing whether the employee had committed any act justifying his immediate dismissal.⁵⁶
- [72]. On other occasions, the Data Protection Act is not relied on by the court. In two recent cases, the Labour Court of Mons held that evidence leading to the dismissal of the employee had been obtained in violation of the right of the employee to respect for his/her private life, guaranteed by Article 8 of the European Convention on Human Rights, and was consequently unlawful.⁵⁷ These decisions did not address the application of the Data Protection Act, though its violation had also been invoked by the plaintiffs. It should be noted that there seem to be important differences between the European Convention and the Data Protection Act, and notably that the Act requires the employer to specifically inform his employees of any control and processing of data, while Article 8 of the European Convention only requires that the control itself be lawful. By rejecting the evidence in the basis of Article 8 only, and by not

2007, available at www.privacycommission.be/fr/static/pdf/annual-reports/rapport-annuel-2007.pdf (12.01.2009) (French).

⁵⁶ Belgium/Labour Court of appeal of Brussels (14.12.1994), *Chroniques de droit social*, 2006, p. 143; Belgium/Labour Court of appeal of Brussels (13.09.05), *Computerrecht*, 2006, p. 100.

⁵⁷ Belgium/Labour Court of Mons (22.05.2007) and Belgium/Labour Court of Mons (18.02.2008), *Revue du droit des technologies de l'information*, 2008, pp. 244-258, with comments K. ROSIER & S. GILSON.

going further and analysing the question of a violation of the Data Protection Act, the court missed an opportunity to order the suppression of the collected data and the prohibition of any further use.

- [73]. A specific issue is the use of data relating to a person's health by the employer. According to Article 7 § 1 of the Data Protection Act the processing of such data is in principle prohibited. However, Article 7 § 2 provides for a limitative list of exceptions to this principle. One of the exceptions is the processing of personal data when it is necessary for the controller of the processing to execute his specific rights and obligations in the field of labour law (point b). This is the case when the employer processes health data in order, for instance, to respect obligations in the framework of the law on labour contracts, *e.g.* in case of suspension of the contract because of incapacity. Another exception concerns processing necessary for preventive medicine, as long as a professional in health care is supervising the processing (point j). Processing of health data that is allowed under the exception clause, has to respect all conditions required for any processing of personal data.⁵⁸

⁵⁸ E. PLASSCHAERT (2005) 'La protection des données personnelles dans le cadre du contrôle des prestations de travail, in: *Vie privée du travailleur et prérogatives patronales*, Brussels: Éditions du Jeune Barreau de Bruxelles, p. 109.

4. Rights Awareness

- [74]. In its management plan of 2003, the CPPL mentions that it wants to contribute to a better information of both controllers of processings and data subjects.⁵⁹ This may be achieved through responses to requests for information and through an active communication system. A renewed website is one of the channels used to achieve this objective. The CPPL has also published several explanatory notes on various subjects to which it wants to draw attention. A publicity campaign will eventually be launched on the basis of a study of market needs. The CPPL wants to use its influence to promote a balanced approach permitting both to preserve the privacy of citizens and not to deprive them of the positive consequences of modern technologies in information processes.

⁵⁹ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Bestuursplan* (15.10.2003), available at www.privacycommission.be/nl/static/pdf/bestuursplan.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Plan de gestion* (15.10.2003), available at www.privacycommission.be/fr/static/pdf/plan_de_gestion.pdf (24.01.2009) (French).

5. Analysis of deficiencies

5.1. Deficiencies regarding effective data protection

- [75]. There are some uncertainties concerning the scope of the Data Protection Act, and notably the concept of ‘file’. In 1997, the Court of Cassation stated that the concept of a ‘file’ in the sense of the Data Protection Act required a logical structure in which a set of personal data is constituted and conserved, so as to allow for a systematic consultation of it.⁶⁰ However, the Act of 11.12.1998 changed the definition of ‘file’, which now reads: ‘any structured whole of personal data accessible following certain criteria’.⁶¹ Although the aim of the new legislation was to generally exclude non-automated processings from its scope, this does not exclude that manual files can be concerned, as long as they constitute a structured whole allowing processing following certain criteria.⁶²

5.2. Deficiencies regarding effective institutions

- [76]. The CPPL still is a largely reactive organisation, since external factors determine its activities, such as demands for an advice or for an authorisation, declarations made by the responsible of a processing, complaints, etc. In recent years, however, some improvements have been made in this field. As far as controls are concerned, the CPPL noted in its annual activity report of 2007 that by then most controls had been executed by the CPPL at its own initiative. In 66 per cent of the cases, the controls and inspections

⁶⁰ Belgium/Court of Cassation (16.05.1997), available at <http://jure.juridat.just.fgov.be/?lang=fr>.

⁶¹ Article 1 § 3 of the Data Protection Act, amended by Belgium/Wet tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens (11.12.1998), *Moniteur belge* (03.02.1999), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) Dutch; Belgium/Loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (11.12.1998), *Moniteur belge* (03.02.1999), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁶² Th. LEONARD & Y. POULLET ‘La protection des données à caractère personnel en pleine (r)évolution’, *Journal des Tribunaux*, 1999, p. 371. See above, no. [50].

were generally focused on one particular sector.⁶³ In 2007, three sectors in particular received attention, namely those of the energy suppliers, the financial institutions and the digital television suppliers.

5.3. Suggestions to fill or reduce these deficiencies

- [77]. The questions concerning the exact scope of the Data Protection Act should be resolved by the legislator in order to increase legal certainty.
- [78]. The CPPL should continue to improve its proactive attitude.

⁶³ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, *Jaarverslag 2007*, available at www.privacycommission.be/nl/static/pdf/annual-reports/jaarverslag-2007.pdf (24.01.2009) (Dutch); Belgium/Commission de la protection de la vie privée, *Rapport annuel 2007*, available at www.privacycommission.be/fr/static/pdf/annual-reports/rapport-annuel-2007.pdf (24.01.2009) (French).

6. Good practices

[79]. It may be recalled that specialised sector committees have been created by law within the CPPL, in order to relieve the CPPL from having to overview the processing of personal data in various specific sectors or with respect to specific systems of data processing. According to Article 31bis § 2 of the Data Protection Act, these committees are composed in equal shares of members of the CPPL and experts chosen for their practical knowledge in the concerned sector. Currently, six sector committees have been created, namely for the sector of social security and health⁶⁴, for the national register of natural persons⁶⁵, for the federal administration⁶⁶, for the central data bank for undertakings⁶⁷, for the

⁶⁴ Belgium/Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (15.01.1990), *Moniteur belge* (22.02.1990; errata, *Moniteur belge* (02.06.1990) & *Moniteur belge* (02.10.1990)), available at www.ejustice.just.fgov.be/wet/wet.htm, consolidated version (29.03.2007) available at www.privacycommission.be/nl/static/pdf/wetgeving/wet_kruispuntbank_sociale_zekerheid.pdf (24.01.1999) (Dutch); Belgium/Loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (15.01.1990), *Moniteur belge* (22.02.1990; errata, *Moniteur belge* (02.06.1990) & *Moniteur belge* (02.10.1990)), available at www.ejustice.just.fgov.be/wet/wet.htm, consolidated version (29.03.2007) available at www.privacycommission.be/fr/static/pdf/wetgeving/loi_banque_carrefour_securite_sociale.pdf (24.01.2009) (French).

⁶⁵ Belgium/Wet tot regeling van een Rijksregister van de natuurlijke personen (8.08.1983), *Moniteur belge* (21.04.1983), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi organisant un registre national des personnes physiques (8.08.1983), *Moniteur belge* (21.04.1983), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁶⁶ Belgium/Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (08.12.1992), *Moniteur belge* (18.03.1993), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁶⁷ Belgium/Wet tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen (16.01.2003), *Moniteur belge* (05.02.2003), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi portant création d'une Banque-carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions (16.01.2003), *Moniteur belge* (05.02.2003), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

judicial information system ‘Phenix’⁶⁸ and for the sector of public statistics.⁶⁹

- [80]. Video surveillance is a relatively new, but already widespread phenomenon, both in public and in private places. On 02.03.2005 the Court of Cassation had to review the conviction of an employee, caught in the act of not registering in a cash register the total amount of the price paid by the customers. The Court held that the video surveillance, as long as it was aimed at the cash register, did not reveal either directly or indirectly any information relating to the cashier, on the basis of any of the distinctive elements mentioned in the Data Protection Act, so that this Act did not apply.⁷⁰ This gap was filled by the legislator, by an Act of 21.03.2007.⁷¹ As soon as a surveillance camera is installed in the framework of prevention of infringements and nuisances or maintenance of public order, the provisions of the new camera law have to be respected. The new legislation concretely sets principles similar to those of the Data Protection Act and provides clear rules for control and information. The Act notably explains the manner by which the images may be watched and radically prohibits exploiting certain sensitive data. Prior to the installation of a surveillance camera, a specific declaration has to be made with the CPPL. This declaration is published, as part of a public register held by the CPPL.

⁶⁸ Belgium/Wet tot oprichting van het informatiesysteem Phenix (10.08.2005), *Moniteur belge* (01.09.2005), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi instituant le système d’information Phénix (10.08.2005), *Moniteur belge* (01.09.2005), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁶⁹ Belgium/Wet betreffende de openbare statistiek (04.07.1962), *Moniteur belge* (20.07.1962), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi relative à la statistique publique (04.07.1962), *Moniteur belge* (20.07.1962), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

⁷⁰ Belgium/Court of Cassation (02.03.2005), with opinion advocate general D. VANDERMEERSCH, available at <http://jure.juridat.just.fgov.be/?lang=fr>.

⁷¹ Belgium/Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's (21.03.2007), *Moniteur belge* (31.05.2007), available at www.ejustice.just.fgov.be/wet/wet.htm (24.01.2009) (Dutch); Belgium/Loi réglant l’installation et l’utilisation de caméras de surveillance (21.03.2007), *Moniteur belge* (31.05.2007), available at www.ejustice.just.fgov.be/loi/loi.htm (24.01.2009) (French).

7. Miscellaneous

- [81]. Recently, some interesting debates on data protection have taken place in Belgium. One of them concerned a federal Act promulgated on 21.08.2008 and organising a platform called ‘e-health’.⁷² The ‘e-Health Platform’ is a public institution that will organise an electronic exchange of medical and other data between health care professionals and institutions, in order to simplify and improve the health care system. The system also allows for the transmission of electronic prescriptions of pharmaceutical products. Doctors, hospitals, health insurance funds and some social security institutions will have access to the system and will even be obliged to provide the platform with certain data. Some organisations of doctors protested that the privacy of patients was not sufficiently protected, notably because health insurance funds and social security institutions will have access to the platform. Asked to give an opinion on the bill, the CPPL, however, did not raise any major objection.⁷³ A royal decree is needed before the Act can enter into force.
- [82]. Another important debate is still going on in the Parliament. It concerns the possible creation of a national databank to be held by the police. In accordance with the Data Protection Act, the police may collect personal data and information presenting a concrete interest for the execution of its mission of administrative and judiciary police. Such data would be collected in a national general databank following modalities to be established by a royal decree. After a first draft proposed by the federal Minister of Justice, the federal Minister for the Interior recently issued a new draft royal decree establishing these modalities. It was generally accepted that a royal decree was needed to organise the policeman’s work and to prevent disrespect for private life. However parliamentarians raised concerns about the procedure followed by the minister, since no political debate had taken place on this issue and the decree’s

⁷² Belgium/Wet houdende oprichting en organisatie van het eHealth-platform (21.08.2008), *Moniteur belge* (13.10.2008), available at www.ejustice.just.fgov.be/doc/rech_f.htm (24.01.2009) (Dutch); Belgium/Loi relative à l’institution et à l’organisation de la plateforme eHealth (21.08.2008), *Moniteur belge* (13.10.2008), available at www.ejustice.just.fgov.be/doc/rech_f.htm (24.01.2009) (French)

⁷³ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 14/2008 (02.04.2008), available at www.privacycommission.be/nl/docs/Commission/2008/advies_14_2008.pdf (24.01.2009) (Dutch); Commission de la protection de la vie privée, Avis no. 14/2008 (02.04.2008), available at www.privacycommission.be/fr/docs/Commission/2008/avis_14_2008.pdf (24.01.2009) (French).

content was too fuzzy. Indeed, the field of application of the databank included any life habit of people belonging to an ethnical group, religious or political convictions, sexual practices, consumer habits. The CPPL issued a mitigated opinion on a draft on 24.09.2008.⁷⁴ The Minister of Justice agreed to have a discussion on the most sensitive issues and to consider the tabling of a bill which would then allow for a parliamentary debate.⁷⁵

⁷⁴ Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2008 (24.09.2008), available at www.privacycommission.be/nl/docs/Commission/2008/advies_33_2008.pdf (24.01.2009) (Dutch); Commission de la protection de la vie privée, Avis no. 33/2008 (24.09.2008), available at www.privacycommission.be/fr/docs/Commission/2008/avis_33_2008.pdf (24.01.2009) (French).

⁷⁵ Belgium/House of Representatives, *Compte rendu intégral*, CRIV 52 PLEN 058 (23.10.2008), pp. 16-24, available at www.lachambre.be/doc/PCRI/pdf/52/ip058.pdf (24.01.2009).

Annexes

Annex 1 – Tables and Statistics ⁷⁶

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	1,168,000€	1,222,000€	Not determined since the budget depended on the Public Federal Service of Justice which has not communicated the part of its budget dedicated to the CPPL	Not determined since the budget depended on the Public Federal Service of Justice which has not communicated the part of its budget dedicated to the CPPL	3,977,300€	4,368,000€	4,606,000€	5,340,000€

⁷⁶ The information in these tables is taken from the annual reports of the CPPL, available on its website www.privacycommission.be/nl (Dutch) (24.01.2009) or www.privacycommission.be/fr (French) (24.01.2009).

Staff of data protection authority	Staff 28	Staff 19	Staff 17	Staff 24	Commission 16 members Staff 49 people	Commission 16 members Staff 41 people	14	16
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	Not available	Not available	4 opinions	3 opinions				3 opinions, 3 recommendations, 3 control procedures initiated
Number of data protection registrations	Not available	Not available	535	657	1,113	1,821	2,037	4,849

Number of data protection approval procedures	Not available	Not available	Not available	Not available	Subdivided following specific committees	156	35	5
Number of complaints received by data protection authority	733	1,085	582	686	678	1,029	1,117	1,538
Number of complaints upheld by data protection authority	Not available	Not available	Not available	Not available	Not available	Not available	31%	110 cases
Follow up activities of data	Not available	Not available	Not available	Not available	Not available	Settlement	Settlement	Settlement 110

protection authority, once problems were established						203 cases Information 628 cases	31% No infringement 8% Inadmissible complaints because the plaintiff has not submitted the requested information or a judicial procedure has been launched 45% Not within the competence of the CPPL 16%	cases No infringement 10 cases Inadmissible complaint 51 cases Others 10 cases Not within the competence of CPPL 64 cases
Sanctions and/or compensation payments in data protection	President of the Court of First Instance of Nivelles	President of the Court of First Instance of Nivelles	Not available	Not available	Not available	Not available	Not available	Not available

cases	decided on 19.12.2000 that he was not competent to decide on remedy	confirmed he his not competent to decide on remedy in a decision on 28.10.2003						
Range of sanctions and/or compensation in your country	Not available	Not available	Not available	Not available	Not available	Not available	Not available	Not available

Annex 2 – Case Law

Case no. 1

Case title	L. v. ASBL Congrégation chrétienne des témoins de Jéhovah
Decision date	06.02.2006
Reference details	No. 2006/15 Cour d'Appel de Liège – Court of Appeal of Liège, <i>Jurisprudence de Liège, Mons et Bruxelles</i> , 2006, pp. 665-667.
Key facts of the case	The plaintiff is a former member of a non-profit Christian congregation for Jehovah witnesses. After he is excluded from the community, he asks the responsible of the community to communicate him a copy of the data concerning him, which is refused. He consequently complains to the CPPL which advises him to launch a judicial complaint. The plaintiff thereupon files a claim, asking for information and suppression of the data. The first instance judge dismisses the claim because the documents detained by the defendant do not correspond to 'files' and are not protected by the Data Protection Act. The plaintiff appeals. He considers the data to be included within the scope of the Data Protection Act.
Main reasoning/argumentation	The court of appeal holds that, according to the Data Protection Act, amended by the Act of 11.12.1998, a file is a structured whole of personal data accessible following certain criteria. Letters and reports do not correspond to this definition but some documents mentioned by the plaintiff may be considered as files. Nevertheless, these documents have either been erased or already communicated to the plaintiff.
Key issues (concepts, interpretations) clarified by the case	Definition of a file as a structured whole of personal data accessible following certain criteria.

Results (sanctions) and key consequences or implications of the case	This case is interesting for its approach to the concept of ‘file’.
Proposal of key words for data base	Private life – File – Structured whole – Letters or reports – Manual file

Case no. 2

Case title	ING België NV / 1. Beroepsvereniging van zelfstandige bankagenten; 2. Federatie voor Verzekerings- en Financiële Tussenpersonen
Decision date	15.02.2005
Reference details	No. 2005/1047 Hof van Beroep te Brussel – Court of Appeal of Brussels, <i>Computerrecht</i> , 2005, p. 139, available at http://www.computerrecht.nl .
Key facts of the case	A company specialised in financial products and insurances is composed of a net of agencies managed by both employees and independent agents. Two independent agencies have bad results. The company thereupon requests from these agencies communication of the data relating to their clients who have withdrawn deposits, so that the company would be able to contact them and to ask them why they take their money out of these agencies. These agents contact associations representing independent bank agents, which launch a procedure against the company.
Main reasoning/argumentation	The plaintiffs argue that communication of the said personal data would be illegal, since it would not satisfy the quality requirements set out in Article 4 of the Data Protection Act, nor would it respect Article 5 of the Data Protection Act, namely the data have to be processed according to an explicit and legitimate finality. The company does not have the right to ask an agency to transmit personal data of its clients in order to control the agency itself, as this finality has never been declared to the clients.

Key issues (concepts, interpretations) clarified by the case	The court bases its decision on an interpretative doctrine of legitimate expectations of the clients concerned. It verifies whether a client can reasonably expect its data to be used for a different finality than the ones originally announced. The court decides that the use of data to control third persons, namely the agents of the bank company, is not a reasonable expectation of the clients, and concludes that the finality is not legitimate.
Results (sanctions) and key consequences or implications of the case	The court orders the bank company to cease its practice under penalty of a payment of 10,000 € in case of new violation after the notification of the decision. This case describes the principle of finality in the context of the control of bank agencies by a bank company. Personal data of the agencies' clients may not be used for such control.
Proposal of key words for data base	Trade practices – Action by professional groups – Processing of personal data – Finality – Private life

Case no. 3

Case title	L.C. / Company X
Decision date	11.06.2004
Reference details	Tribunal de Première Instance de Bruxelles – Court of First Instance of Brussels, <i>Bulletin des Assurances</i> , 2005, p. 47.
Key facts of the case	The plaintiff has subscribed a motor vehicle liability insurance covering several risks among which theft. His car has been stolen and he has asked for an indemnity. The insurer has refused to indemnify because of doubts on the plausibility of the theft. The insurer has informed the plaintiff about the resolution of the contract and has also informed a risk assessment company of its doubts relating to the plaintiff. The plaintiff is registered in the “special risks” file of that company.

Main reasoning/argumentation	The plaintiff files a claim against the insurer. He asks an order against the insurer to pay the indemnity foreseen in the insurance contract and to repair the material and moral prejudice following his registration in the file processed by the risk assessing company. Indeed, this registration has led to the impossibility to find a new insurer.
Key issues (concepts, interpretations) clarified by the case	The court has to pronounce itself on the conformity of data processing by a risk assessment company.
Results (sanctions) and key consequences or implications of the case	The court decides that the theft was real, and orders the insurer to pay the corresponding indemnity. However, it rejects the second claim, holding that the file processed by the risk assessment company complied with the Data Protection Act. Indeed, the finality is legitimate (namely the struggle against fraud), the processing is necessary and proportionate, the data are correct, pertinent and not excessive, and there are no express discriminatory or outrageous words on the plaintiff.
Proposal of key words for data base	Data Protection Act – Legitimacy of the finality – Exactness of data – Non-discriminatory and non outrageous character

Case no. 4

Case title	Serwy & Wengler / Union professionnelle du crédit
Decision date	22.03.1994
Reference details	Président du Tribunal de Première Instance de Bruxelles, siégeant comme en référé – Voorzitter van de Rechtbank van eerste Aanleg te Brussel, zetelend zoals in kort geding - President of the Court of First Instance of Brussels, sitting as in interim proceedings, <i>Journal des Tribunaux</i> , 1994, p. 841.

Key facts of the case	The first plaintiff is the manager of a bank agency; the second plaintiff is his wife. The agency enters into a commercial leasing contract with the bank, relating to a car, and the plaintiffs act as guarantors. When a dispute arises between the agency and the bank, the latter communicates the coordinates of the plaintiffs to a risk assessment company.
Main reasoning/argumentation	The plaintiffs contest the exactness of the data. They file a claim on the basis of Article 14 of the Data Protection Act, in order to obtain that the risk assessment company be ordered to erase the data, to communicate the correction to its members and to pay a compensation for non-material damage.
Key issues (concepts, interpretations) clarified by the case	The right to be informed guaranteed by the Data Protection Act is fundamental and allows every citizen to control if information is exact, complete and pertinent. The controller of the processing has to proceed carefully and has to be constantly attentive to the finality of the processing. He may not simply reproduce data supplied by third parties, but has to verify if it is not premature to process them.
Results (sanctions) and key consequences or implications of the case	The president of the court orders the risk assessment company to erase the data, and to inform its clients of the suppression of the data. It is interesting to note that the president also awards an indemnity for non-material damage of 50,000 BF (+/- 1,250 €) for the husband and 50,000 BF (+/- 1,250 €) for the wife. Scholars have criticised this part of the judgment, arguing that the procedure under Article 14 of the Data Protection Act does not allow for measures other than those mentioned in that provision.
Proposal of key words for data base	Data Protection Act – File – Suppression – Damages