FRA

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

Luxembourg, Luxembourg
February 2009

Contents

Executive summary

Overview

[1]. The notion of data protection is relatively new in Luxembourg. Until the entry into force of the 2002 Law, there was no real data protection 'culture', tradition or education. The one law somewhat covering the field was the Law of 31 March 1979 governing the use of personal data in information technology processing that covered databases, but it was hardly applied and provided for a commission that was consultative only. The law of 31 March 1979 was repealed by the 2002 Law.[1]

[2]. There is no specific constitutional right to the protection of one's personal data embodied in the Luxembourg Constitution. However, the Luxembourg Constitution guarantees the right to privacy and the inviolability of written communications, regardless of their format.[2]

Data Protection Authority

[3]. The *Commission nationale pour la protection des données* (CNPD) [National Data Protection Commission], Luxembourg's DPA, was created at the end of 2002. The CNPD is an independent collegial body charged with monitoring that personal data are being processed according to the 2002 Law and its implementing regulations. It is a public authority established in the form of an *Etablissement Public* [Public Institution]. It has financial and administrative autonomy under the supervision of the Minister of Communications, and carries

[1] Luxembourg/*Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques* (31.03.1979), Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 44(1) , interview of 08.01.2009 with CNPD member, CNPD (2008) *Law of July 27th 2007 : Major changes & Clarifications*, at page 1, available at http://www.cnpd.lu/objets/publications/autres_publications/0508_law_changes.pdf (01.06.2009).

[2] Luxembourg/*Constitution du Grand-Duché de Luxembourg* Service Central de Legislation, *Constitution du Grand-Duché de Luxembourg, texte à jour au 1er janvier 2008* (01.01.2008), Articles 11(3) and 28, available at : http://www.legilux.public.lu/leg/textescoordonnes/recueils/Constitution/Page_de_garde.pdf, (17.12.2008).

out its duties with complete independence. The CNPD maintains an extensive multilingual website.[3]

Compliance

[4]. In general the registration duties are complied with, but the CNPD cannot usually be aware of non-compliance unless a complaint is lodged. This applies particularly with respect to surveillance. Given the number of notifications/declarations the CNPD has to process and the simplified notification procedure, it is more difficult to detect if a notification has not been filed. It is usually easier to detect non-compliance with prior authorization requirements, as that is a more visible violation of the requirement, particularly with respect to video surveillance. Also, given that the sanctions the CNPD can impose are primarily administrative, there can at times be a compliance problem.[4]

Sanctions, Compensation and Legal Consequences

[5]. At this time, enforcement of data protection legislation through sanctions and/or compensation payments in Luxembourg depends largely on the personal initiative, and complaints, of data subjects. Data subjects are informed of their rights by the CNPD, the CNPD's extensive website, and the Luxembourg Consumer's Union. The financial burden of legal procedures regarding data protection in Luxembourg are borne by the State only in criminal cases, otherwise the financial burden is shared by the parties. To date, however, there have not been many data protection cases in Luxembourg.[5]

[3] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34., and http://www.cnpd.lu/fr/.

[4] Interview of 08.01.2009 with member of the CNPD.

[5] Interview of 08.01.2009 with member of the CNPD.

Rights Awareness

[6]. There are no other studies and surveys on awareness regarding data protection law and rights in the Luxembourg other than the two 2008 Eurobarometer surveys.[6]

Analysis of deficiencies

[7]. During its short time in existence, the CNPD has concentrated its efforts on informing the relevant parties of their rights and responsibilities. Major deficiencies in Luxembourg's data protection regime may appear in time, but at this point there are no major deficiencies.[7]

Good Practice

[8]. One example of a good practice is the CNPD's decision in the Mondorf case in which the CNPD authorised Mondorf Thermal Spa's second request for authorisation of a member biometric data recording/surveillance system (fingerprints), after denying a prior request (see also Annex 2c – Case Law).[8]

Miscellaneous

[9]. In December of 2008, the Law on cooperation between fiscal administrations was passed into law. The law provides for the exchange of information through data interface among several administrative entities. The stated purpose of the law is to ensure recovery of tax payments, fight tax fraud and guarantee equality of citizens and companies with regard to taxation.[9]

---

6 Interview of 08.01.2009 with member of the CNPD.

7 Interview of 08.01.2009 with member of the CNPD.

8 CNPD (2006) *Déliberation no. 33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques* [Deliberation No. 33/2006 of 12 April 2006 of the CNPD on Domaine Thermal de Mondorf's prior authorization request for surveillance using biometric data], and Interview of 08.01.2009 with member of the CNPD.

9 Luxembourg/*Loi du 19 décembre 2008 ayant pour objet la cooperation interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions Directes, de*

1. Overview

[10]. Below is Luxembourg's status with respect to the applicable European, international and domestic data protection standards and instruments:

EU

1. Directive 95/46/EC of 24 October 1995 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 – transposed into domestic law by the Law of 2 August 2002 on the protection of individuals with regard to the processing of personal data;[10]

2. Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector – transposed into domestic law by the Law of 30 May 2005 on personal data processing in electronic communications.[11]

3. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) – this directive has not yet been entirely transposed into Luxembourg national law (see 2005 Law).

Council of Europe

1. Article 8, European Convention on Human Rights – open for signature and signed on 04.11.1950, ratification and entry into force on 03.09.1953;

2. Basic Principles contained in Appendix to Recommendation Rec(87)15 by Committee of Ministers to Council of Europe Member States regulating use of personal data in the police sector, adopted by

l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises (19.12.2008).

[10] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002).

[11] Luxembourg/*Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques* (30.05.2005).

Committee of Ministers 17.09.1987 – we have not found evidence that these are taken into account.

3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – open for signature and signed on 28.01.1981, ratified on 10.02.1988, entry into force on 01.06.1988;

4. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow – open for signature on 08.112001, signed on 24.02.2004, ratified on 23.01.2007, entry into force on 01.05.2007; and

5. Convention on Human Rights and Biomedicine – open for signature and signed on 04.04.1997, but not ratified.

UN

1. Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and the General Comment No. 16 on Article 17 ICCPR (para. 10 on personal data) – ratified on 18 November 1983, and

2. The Guidelines for the Regulation of Computerised Personal Data files adopted by a resolution of the General Assembly of the United Nations on 14 December 1990, adopted without vote[12] - we have not found evidence that these are taken into account in Luxembourg legislation.

Luxembourg

1. Constitution of the Grand Duchy of Luxembourg – Articles 9-31 deal with civil liberties and fundamental rights; Article 11(3) provides for the right to privacy (more details below);[13]

2. Law of 11 August 1982 on the protection of the right to privacy;[14]

3. Law of 2 August 2002 on the protection of individuals with regard to the processing of personal data, as amended by the 2007 Law cited

[12] Available at: http://www.un.org/documents/ (30 January 2009.

[13] Luxembourg/*Constitution du Grand-Duché de Luxembourg* Service Central de Législation, *Constitution du Grand-Duché de Luxembourg, texte à jour au 1er janvier 2008* (01.01.2008), Article 11(3) available at : http://www.legilux.public.lu/leg/textescoordonnes/recueils/Constitution/Page_de_garde.pdf, (17.12.2008).

[14] Luxembourg/*Loi du 11 août 1982 concernant la protection de la vie privée* (11.08.1982).

below (unless otherwise specified, the consolidated text is herein referred to as the '2002 Law'), transposes Directive 95/46/EC;[15]

4. Law of 8 June 2004 on freedom of expression in the media, as amended (the '2004 Law');[16]

5. Law of 30 May 2005 relative to specific provisions for individuals regarding processing of personal data in the electronic communication sector, as amended (the '2005 Law'), transposes Directive 2002/58/EC (part of telecommunications package);[17] and

6. Law of 27 July 2007 modifying, among others, the Law of 2 August 2002 cited above (the '2007 Law'), transposes Directive 95/46/EC and included in the consolidated text of the 2002 Law.[18]

[11]. There is no specific constitutional right to the protection of one's personal data. As stated above, however, Article 11(3) of the Luxembourg Constitution guarantees the right to privacy. The guarantee of this right is subject only to exceptions set forth by law. Moreover, Article 28 provides that the confidentiality of letters (broadly interpreted to mean all written communications, regardless of the format) is inviolable.[19]

[12]. The notion of data protection is relatively new in Luxembourg. Until the entry into force of the 2002 Law, there was no real data protection 'culture', tradition or education. The one law somewhat covering the field was the Law of 31 March 1979 governing the use of personal data in information technology processing. That law covered mainly databases, was hardly applied and provided for a commission that was

15 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002).

16 Luxembourg/*Loi du 8 juin 2004 sur la liberté d'expression dans les médias* (08.06.2004).

17 Luxembourg/*Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard tu traitement des données à caractère personnel dans le secteur des communications électroniques, etc.* (30.05.2005).

18 Luxembourg/*Loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, etc*. (27.07.2007).

19 Luxembourg/*Constitution du Grand-Duché de Luxembourg* Service Central de Legislation, *Constitution du Grand-Duché de Luxembourg, texte à jour au 1er janvier 2008* (01.01.2008), Articles 11(3) and 28, available at : http://www.legilux.public.lu/leg/textescoordonnes/recueils/Constitution/Page_de_garde.pdf, (17.12.2008).

consultative only. The law of 31 March 1979 was repealed by the 2002 Law.[20]

[13]. The span of time between the 31 March 1979 touching on subjects somewhat related to data protection, and the passage of the 2002, 2004 and 2005 Laws some 20 years later, is testimony to the sudden increase of awareness in Luxembourg of the need to protect privacy and personal data, brought to a head by the increased use of information technology. Accompanying the awareness of the need to protect privacy was a growing consumer protection movement.[21]

[14]. Another law, the Law of 11 August 1982 on the protection of the right to privacy, continues to govern the right to privacy in Luxembourg to some extent. That law provides for imprisonment of eight days to one year and a fine of EUR 251 to 5,000, or either one of those sanctions, for whomever intentionally infringes the right to another's privacy through opening a sent or transmitted sealed message without the consent of the addressee or sender. The same sanction applies to whomever becomes informed of the content of that message by any other medium or device, or erases such a message.[22]

[15]. Moreover, Luxembourg's Penal Code provides for criminal sanctions in the form of imprisonment of eight days to one month and a fine of 251 to 2,000 EUR, or either one of these sanctions alone upon conviction of having removed a letter put into the post, or opened the letter in order to violate the confidentiality of that letter.[23]

[16]. Luxembourg's primary pieces of data protection legislation are the 2002 Law (meaning the consolidated text as modified by the 2007 Law), the 2004 Law and the 2005 Law.

The 2002 Law

---

[20] Luxembourg/*Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques* (31.03.1979), Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 44(1) , interview of 08.01.2009 with CNPD member, CNPD (2008) *Law of July 27th 2007 : Major changes & Clarifications*, at p. 1, available at http://www.cnpd.lu/objets/publications/autres_publications/0508_law_changes.pdf (01.06.2009).

[21] C. Pierre-Beausse (2005) *La Protection des Donneés Personnelles* [Personal Data Protection], Luxembourg : Editions Promoculture.

[22] Luxembourg/*Loi du 11 août 1982 concernant la protection de la vie privée* (11.08.1982), Art. 2(3), and , CNPD (2008) *Processing subject to prior autorisation : Data protection and employment*, at p. 19, available at http://www.cnpd.lu/objets/publications/autres_publications/0508_dp_employement.pdf (01.06.2009).

[23] Luxembourg/*Code pénal Grand-Duché de Luxembourg*, 01.01.2008, Article 460 (01.01.2008).

[17]. The 2002 Law directly transposes virtually all of Directive 95/46/EC's definitions and substantive provisions. However, it adds further detail to some definitions while adding some definitions not in the Directive. For example the definition of personal data specifies that 'any information' includes all information regardless of its format, including sound and images, and adds the factor of genetic identity to those listed as specific to the 'data subject' definition. To the definition of 'third party' a sentence providing that 'in the public sector a third party is understood to be a ministry, administration, public establishment, local government or government agency other than the controller or processor'.[24] The definition of data subject's consent also includes consent given by the data subject's legal representative.[25]

[18]. Additional definitions in the 2002 Law include the following:

1. 'code of conduct' – contributions from all sectors aimed at proper application of the law. The codes of conduct are written at the national level or EC level by the professional associations or other organisations that represent the controllers and are optionally put for approval before the National Commission or group that protects persons with respect to processing of personal data, as established by Article 29 of Directive 95/46/CE;

2. 'National Commission' – National Data Protection Commission;

3. 'health data' – any information concerning the physical and mental state/condition of a data subject, including genetic data;

4. 'genetic data' – all data concerning the hereditary characteristics of an individual or group of related individuals;

5. 'medical authority' – any health practitioner and person subject to the same obligation of professional secrecy, as well as any hospital governed by the Law of 28 August 1998 on hospitals, carrying out data processing for the purposes of preventive medicine, medical diagnosis, the administration of healthcare, treatments, or health service management;

6. 'minister' – the minister charged with data protection;

7. 'social security body' – any public or private law body that provides mandatory or optional services related to disease/illness, maternity, old

[24] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 2.

[25] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 2.

age, personal injury, disability, addiction, death, unemployment, parental leave, as well as any other family or social assistance services;

8. 'third country' – a country that is not an EU Member State; and

9. 'supervision' – any activity that is carried out by means of technical instruments and consists of the observation, collection or recording, on a regular basis, of the personal data of one or several persons, related to the behaviour, movement, communication or the use of electronic or computerized devices.[26]

[19]. The 2002 Law's scope of application is stated in the affirmative and applies to data processing regarding public security, defence, criminal pursuit activities or State security, even when linked to an important economic or financial State interest, without prejudice to the national and international legal provisions governing those areas. The 2002 Law is silent with respect to the controller's obligation to take the necessary measures to ensure that each of the establishments complies with the applicable national law when the same controller is established in the territory of several Member States.[27]

[20]. The Luxembourg data quality provisions vary slightly from those of the Directive. Whereas the Directive provides that further processing or storage for longer periods than necessary are permissible for historical statistical or scientific purposes and use,[28] the 2002 Law simply states that further processing for those purposes and uses is not incompatible with the purposes for which the data were originally collected. And, the 2002 Law provides for sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions, for violation of Article 4 of the 2002 Law. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[29]

[21]. The provisions regarding legitimating data processing are substantially identical to those in the Directive. Violation of those provisions incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the

[26] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 2.

[27] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 3(1).

[28] Council Directive 95/46/EC (24.10.1995), Art. 6(b) and (c).

[29] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 4.

data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[30]

[22]. The provisions regarding processing of special categories of data include the specification that genetic data are included in the categories of data related to health and sex life the processing of which is prohibited. Public interest exceptions to those restrictions exist, however, most notably for the processing of historical, statistical or scientific data. Violation of those provisions incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or a combination of both. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[31]

[23]. The 2002 Law contains an article dealing exclusively with the processing of special categories of health-related data which provides that:

> Processing of data related to health and sex life necessary for the purpose of research in health or scientific research can be carried out by health professionals, as well as by research organisations and physical or legal persons whose research project has been approved under the applicable biomedical research legislation. If the responsible authority is a legal person, it must disclose the appointed delegate subject to the obligation of professional secrecy.

The article goes on to specify the bodies subject to professional secrecy, the required safeguards for the processor and the applicable legislation. Violation of those provisions incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[32]

[24]. The 2002 Law also contains an article dealing exclusively with the processing of judicial data. The article basically sets forth the provisions of the Directive's Article 8, para. 5. Violation of those provisions in the private sphere incurs sanctions of eight days to one

[30] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 5.

[31] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 6.

[32] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 7.

year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[33]

[25]. Article 9 of the Law of 2002 is devoted to personal data processing in the context of freedom of expression in which it adopts Article 9 of the Directive, without prejudice to the 2004 Law (described below). Data processing solely for journalistic purposes, or the purpose of artistic or literary expression is not prohibited under the provisions regarding special categories of data, neither is the processing of judicial data prohibited for those purposes.

[26]. Additionally, when the processed data is data made public by the data subject, data having a direct relationship with the public life of the data subject or with an event or fact in which the person is voluntarily involved, the processing is not subject to the requirement for adequate safeguards. These include those for data being transferred to third countries; the obligation to inform the data subject when the data subject's right to information would compromise the collection of data, the proposed publication, making available to the public, or any manner of allowing the identification of the information sources; or, to the data subject's limited right of access as provided in Article 29 of the 2002 Law (see below).[34]

[27]. Article 10 of the 2002 Law deals with data processing for surveillance purposes. This type of data processing can only be carried out with the consent of the data subject or on the outskirts of any place whether accessible to the public or not, other than residential areas. These areas would include covered parking areas, train stations, airports and public transportation, provided that the place in question is by its very nature, situation, configuration or the kind of people that frequent it, a risk that makes the data processing necessary for the security of its users/travellers, the prevention of accidents, the protection of property (if there is a risk of theft or vandalism). This type of processing could also be permitted in private areas at which the physical or legal person is domiciled if the person is physically or legally incapable of giving consent.[35]

[33] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 8.

[34] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 9.

[35] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 10(1).

[28]. Data subjects are to be informed of the data processing in the above paragraph by the appropriate means such as road signs, circulars and/or mailings sent by registered mail or mass e-mail. Upon the request of the data subject, the controller will provide the data subject with the information listed in Article 26(2) (see below). Data collected for purposes of surveillance are not disclosed unless the data subject has given legally valid consent; the disclosure is made to public authorities under Article 17(1) (see below); or, to judicial authorities competent to observe or pursue a criminal offence, and to judicial authorities before whom a legal right is being defended or exercised.[36]

[29]. Violation of the provisions of Article 10 incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[37]

[30]. If the employer is the controller, data processing for purposes of surveillance at the workplace can only be carried out under the conditions set forth in the Luxembourg Labour Code requiring that the surveillance be carried out with the prior approval of the CNPD, and that the processing be necessary for:

(1) workers' security and health needs;

(2) the company's property protection needs;

(3) inspection of the production process solely relating to machines;

(4) temporary inspection of the worker's labour/services provided, when such inspection is the only way of determining the exact remuneration; or

(5) in the context of organisation of flextime under the Luxembourg Labour Code.

For numbers 1, 4 and 5 above, the company joint committee, to be set up if necessary, has the power to decide on (1) the introduction or application of technical facilities that would inspect the worker's behaviour and performance on the job, and (2) the introduction and

[36] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 10(2)-(3).

[37] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 10(4).

amendment of measures regarding workers' health and security as well as the prevention or workplace illnesses.

The data subject's consent does not legitimate the employer's processing of the data.

Without prejudice to the data subject's right to information, the employer must give prior notice to the data subject, and for persons falling under the private law contract regime, the joint committee, or if none, the personnel delegation, or if none, *l'Inspection du travail et des mines* [Luxembourg's labour inspectorate]. For persons falling under the statutory regime the employer must give prior notice to the data subject and the bodies representing personnel as provided by the applicable laws and regulations. A violation of these Luxembourg Labour Code provisions is subject to the same sanctions as those for Article 10.[38]

[31]. Chapter III of the 2002 Law corresponds to the Directive's Section IX on notification. Under Article 12, the controller must notify the CNPD of all data processing not related to judicial data, not previously authorised by the CNPD or by Grand-Ducal Regulation. Data processing by the same controller and for the same purposes may be notified only once to the CNPD. Moreover, when a data protection officer is named and that official maintains a register showing the required processing, the processing is exempt from the notification requirement. Further exempt processing is that carried out by lawyers, notaries and bailiffs when related to legal defence; that carried out for purposes of journalism or literary or artistic expression; and that necessary to save the vital interests of the data subject or another person when the data subject is physically or legally incapable of giving his or her consent.[39]

[32]. Article 12 also carves out 14 exemptions to the notification requirement for personal data processing that is:

(a) related exclusively to payroll administration for employees working with or for the controller when the data is used for that purpose and disclosed solely to individuals who have the right to access it;

(b) aimed exclusively at the management of candidacy and recruitment, as well as the administration of personnel working

[38] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 11; Luxembourg/*Code du Travail* (01.10.2008), Art. L. 261-1, L.261-2 and L.423-1.

[39] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 12(1)-(2).

for the controller, as long as there is no health-related or sensitive or judicial data, or data related to evaluation of the data subject, and the data cannot be disclosed to third parties unless done so according to a legal or regulatory provision or if the disclosure is necessary for the purposes of the processing;

(c) related exclusively to the data controller's accounting to the extent that the data are used solely for such accounting and the processing concerns only those persons who are necessary to such accounting. The data cannot be disclosed to third parties, unless done so under a regulation or other legal provision, or to the extent that the data is necessary to the accounting;

(d) aimed exclusively at the administration of shareholders, bondholders and company members, to the extent that the processing is related solely to the data necessary for such administration, that the data are related solely to the persons the data of which is necessary for such administration, that the data are not disclosed to third parties unless done so under a regulation or other legal provision;

(e) aimed exclusively at the management of the data controller's potential, existing or former customers and suppliers, but the data cannot be health-related, sensitive or judicial, and cannot be disclosed to third parties unless done so under a regulation or other legal provision, or for purposes of the normal management of a company;

(f) carried out by a foundation, an association or any other non-profit organisation within the context of its ordinary activities. The processing must be exclusively related to the administration of the organisation's own members, persons with whom the controller has regular contact or the benefactors of the foundation, association or organisation, and such data cannot be disclosed to third parties, unless done so under a regulation or other legal provision;

(g) absolutely necessary for communications with the sole objective of entering into contact with the data subject, as long as the data is not disclosed to third parties and failing any other applicable provision of the 2002 Law;

(h) related exclusively to the registration of visitors when carried out in the context of manual access control, to the extent that the processing is limited to the visitor's name and professional address, his or her employer, vehicle information, as well as the name, section and function of the person visited and the hour of

the visit. Such data shall be used solely for the manual access control;

(i) carried out by teaching institutions with a view to managing their relations with their students. The processing must be related exclusively to personal data of potential, current or future students of the institution concerned and the data cannot be disclosed to third parties, unless done so under a regulation or other legal provision;

(j) carried out for administrative authorities if the processing is subject to applicable legal provisions regulating the access, use and obtaining of such data;

(k) necessary for the management of computer and electronic communication systems and networks, provided that they do not operate for surveillance purposes under the meaning of the 2002 Law;

(l) performed according to the relevant article of the Law of 28 August 1998 on hospitals, except for genetic data processing;

(m) performed by a doctor relating to his or her patients, under the 2002 Law's article allowing medical authorities to process data related to health and sex life necessary for purposes of preventive medicine, medical diagnostics, administration of care and treatment, except for genetic data; and

(n) performed by a pharmacist or professional subject to the Law of 26 March 1992 on the exercise and revaluation of certain healthcare professions. Personal data processing must be related exclusively to the delivery of medicine and care or services provided, and the data cannot be disclosed to third parties, unless done so under a regulation or other legal provision.

The failure to notify as required or the furnishing of incomplete or false information is punishable by a fine ranging from EUR 251 to 125,000. The tribunal asked to adjudicate a matter can order that the illicit data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[40]

[33]. In addition to adopting all of the Directive's provisions regarding the contents of notification, Article 13 of the 2002 Law requires that the basis for the legitimacy of the processing be provided, and provides

[40] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 12(3)-(4).

information on transmission and payment to the CNPD and as well as the simplified notification procedure.[41]

[34]. Article 14 of the 2002 Law requires prior authorization, a more onerous procedure than prior checking, for data processing related to genetic data; recorded surveillance; historic, statistical or scientific purposes; data sharing; the credit and solvency of data subjects when performed by persons other than those financial sector professionals or insurance companies for their clients; biometric data necessary to verify the identity of persons; and the use of data for purposes other than those for which it was collected, unless the data subject's prior consent has been obtained or it is necessary to save the data subject's vital interest. The article further specifies the information required in the authorisation request, the CNPD payment and transmission as well as simplified notification procedure information. Violation of Article 14 incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[42]

[35]. The 2002 Law's Article 15 covers publicising of processing operations. In addition to adopting all of the Directive's provisions, the Article 15 specifies that the register will also include processing previously authorised by the CNPD under the prior authorisation provisions. The register is available online and all information in the notification and prior authorisation requests may be inspected by any person with the exception of the description allowing a preliminary assessment of security measures for such processing. The CNPD may limit publicising when a particular measure is necessary to preserve the State; defence; public security; the fight against money laundering; an important State economic or financial interest; the protection of the data subject or the rights of others; freedom of expression; a public authority's exercise of power; and business secrets or other forms of professional confidentiality. The CNPD's annual report lists the notifications and authorisations.[43]

[36]. Article 16 of the 2002 Law covers data sharing and provides that the CNPD should give prior authorisation for data sharing not expressly provided covered by legal or regulatory provisions. The controllers of the two entities proposing to share data must submit a joint request to

[41] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 13.

[42] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 14.

[43] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 15.

the CNPD. The data sharing should be for legal purposes representing a legitimate interest of the controller; not result in discrimination, or a reduction of the rights, liberties and guarantees of the data subject; and be accompanied with appropriate safeguards. Data sharing can only be authorised for compatible purposes and when any applicable confidentiality obligation is respected.[44]

[37]. Article 17 of the 2002 Law covers authorisation of data processing by Grand-Ducal regulation. The regulations cover general processing necessary for law enforcement agencies such as the Grand-Ducal Police, and the disciplinary bodies of the police and customs and duties administration. They also cover processing related to State security, defence, public security, as well as that involved in criminal law investigation under international accords, intergovernmental agreements or Interpol. Moreover, the use of closed-circuit television in high-risk public areas for protection and law enforcement purposes is governed by Grand-Ducal regulation.[45]

[38]. Monitoring of data processing under national or international law is performed by an authority composed of the State Prosecutor, or an appointed delegate in the matter, and two members of the CNPD that the Minister of Communications names at the suggestion of the CNPD. The CNPD's organisation and functioning are regulated by Grand-Ducal regulation. The CNPD can directly access all data that is the subject of any dispute or about which it performs an investigation. Violation of Article 17 in the private sphere incurs sanctions of eight days' to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[46]

[39]. Articles 18-20 cover personal data transfer to third countries, and essentially adopt all of the Directive's provisions. Whoever unlawfully transfers personal data to a third country incurs sanctions of eight days' to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped

[44] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 16.

[45] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 17(1).

[46] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 17(2)-(3).

under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[47]

[40]. The Directive's confidentiality and security of processing provisions are adopted in Articles 21-23 of the 2002 Law. Additionally, Article 23 of the 2002 Law specifies that security measures must prevent access to data processing facilities, formats, memory, use and access during transport, as well as guarantee the monitoring of data access, transmission, identity of persons accessing data and guarantee saving of the data itself. Moreover, members of the CNPD are subject to an obligation of professional secrecy and data controller and others charged with data processing cannot invoke their obligation of professional secrecy against members of the CNPD acting within the scope of the duties. Violation of the confidentiality and security provisions incurs sanctions of eight days' to six months' imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[48]

[41]. Articles 26-31 of the 2002 Law cover the data subject's rights, adopting the Directive's provisions on information to be given to the data subject, the data subject's right of access to data, right to object and applicable exemptions and restrictions. The 2002 Law further provides that a medical patient has the right to access personal data through a doctor, as does the surviving spouse (when not legally separated from the deceased) and a guardian of a legally incapacitated person. An exception to the data subject's right of access exists when the data is used for journalistic purposes or artistic or literary expression when the data would allow the identification of the source of the data. Subject to this exception, the data subject's right in this context is to be asserted through the CNPD in coordination with the appropriate member of the Press Council (see section below on data protection and freedom of expression). Knowingly violating those provisions incurs sanctions of eight days' to one years' imprisonment and a fine ranging from 251 to 125,000 EUR, or either one of the two sanctions.[49]

[42]. Articles 32-37 provide for the duties and powers of the CNPD which are set forth and analysed in Section 2 below.

---

47 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 18-20.

48 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 21-25.

49 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 26-31.

[43]. Articles 38 and 39 of the 2002 Law provides for an individual's judicial recourse, and liability of the offender when damage is suffered due to an unlawful processing operation. As set forth in Article 39, the remedial action is in the form of injunctive relief that can be brought as follows:

1. At the request of the:

- State Prosecutor bringing a public action for violation of the 2002 Law;

- CNPD when an administrative sanction under Article 33 of the 2002 Law has not been complied with, when recourse has not been sought against that sanction or the sanction has been confirmed by the competent administrative tribunal; or

- injured party when the CNPD has not taken a position or ruled on a petition filed with it.

The head of the District Court in the place where the processing is carried out, or that judge's replacement, shall order the cessation of the processing contrary to the 2002 Law and the temporary suspension of the data controller or processor. The same authority can also order the temporary closure of the establishment of the data controller or processor when their sole activity is that of data processing.

2. The action can be brought even when the illegal processing operation has ended or will no longer be repeated.

3. The action can be brought and adjudicated as an action for summary judgment/interim measures, and cannot be opposed.

4. If a party is not satisfied with an initial sentence, it may request that the competent judicial tribunal order a penalty payment or fine, without prejudice to any possible liability for damages and interest under the applicable Civil Code provisions.

5. Publication in the newspaper or other medium of an entire decision, or an extract thereof, can be ordered at the expense of the offender, provided that the decision is final.

6. The temporary suspension or establishment closure can be ordered independently of the public action brought by the State Prosecutor. Such suspension or closure ends when the action is dismissed or the

accused party is acquitted, or at the latest at the end of two years from the initial suspension or closure decision.[50]

[44]. Article 40 of the 2002 Law covers the possibility for a controller to appoint a data protection officer, the powers of which are to investigate and monitor the controller's compliance with the 2002 Law and its implementing regulations. The data protection officer also has the right to receive information from the controller, and to inform the controller on matters of such compliance. The data protection officer is a natural or legal person who carries out his/her mission and activities independently of the controller. The data protection officer must be certified as such by the CNPD, and a Grand-Ducal Regulation further specifies the data protection officer's duties and activities.[51]

[45]. Finally, the 2002 Law has no specific provisions on codes of conduct other than the definition cited above and the mission under Article 32(3)(g) to receive and, if after discussion with the appropriate entities it deems the proposed code compliant with the 2002 Law, approve it.[52]

The 2004 Law

[46]. The 2004 Law covers freedom of expression in the media with respect to the right to privacy. It makes no reference to any EU directive, and was slightly amended by the 2007 Law to include provisions relating to personal data processing. Those amendments add to the Press Council's (entity that grants and withdraws journalist credentials) duties the obligation to include duties and responsibilities related to personal data processing in the journalist and editor ethics code that it drafts. Moreover, the Press Council is charged with setting up a Complaint Commission that receives complaints from individuals regarding the information diffused in the media. The 2007 Law required that the complaints also include those regarding the respect of rights and liberties of persons with respect to processing of their personal data.[53]

---

50 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 39 and *Luxembourg/Code civil Grand-Duché de Luxembourg* 01.01.2007, Articles 2059 and 2066 (01.01.2007).

51 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 40, and Luxembourg/*Règlement grand-ducal du 27 novembre 2004 concernant le chargé de la protection des données* (27.11.2004).

52 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 2(a) and 36(3)(g).

53 Luxembourg/*Loi du 8 juin 2004 sur la liberté d'expression dans les médias* (08.06.2004), Art. 23, and Luxembourg/*Loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, etc*. (27.07.2007)..

The 2005 Law

[47]. The 2005 Law, part of a Telecommunications Package, transposes Directive 2002/25/EC, and largely mirrors that Directive. The Law adds definitions for the *Institut Luxembourgeois de Régulation* [Luxembourg Regulatory Institute], electronic communications network, public communications network and electronic communications service. Articles 5 and 9 of the 2005 Law were amended to provide for service providers' retention for law enforcement purposes of traffic data and non-traffic data, respectively, for a maximum of six months. This is the one element of the Data Retention Directive that his been transposed into Luxembourg law.[54]

[48]. Without prejudice to the ability of competent law enforcement and judicial authorities to do so, the CNPD is charged with enforcing the 2005 Law and its implementing regulations. Violation of the 2005 Law incurs sanctions of eight days' to six months' imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[55]

[49]. One of the axes of around which Luxembourg's national data protection debate revolves is the protection of personal data in the telecommunications sector. The CNPD just completed an investigation using an outside expert regarding whether the telecommunications department of *l'Entreprise des P&T* (EPT) [the national post and communications entity] was in compliance with the 2002 and 2005 Laws. The investigation found that the EPT took great care to protect its clients' personal data. The CNPD is extending that investigation to private cellular telephone service providers.[56] And, as indicated by the new law mentioned in Section 8, regarding the entry into force of the law on cooperation between fiscal administrations, the respect of privacy and fundamental rights will be a growing concern with regard to the data sharing capabilities of public administration entities.

---

54 Luxembourg/*Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard tu traitement des données à caractère personnel dans le secteur des communications électroniques, etc.* (30.05.2005), Arts. 5 and 9, and d.

55 Luxembourg/*Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard tu traitement des données à caractère personnel dans le secteur des communications électroniques, etc.* (30.05.2005).

56 *Investigation menée dans le secteur des télécommunications* [Telecommunications sector investigation], available at: http://www.cnpd.lu/fr/actualites/activite_nationale/2009/03/10_03_2009/index.html (13.03.2009).

[50]. In a similar vain, another important issue is the extent to which officials of the Ministry of Foreign Affairs and Immigration can have access to the personal data of individuals for purposes of verifying the legality of their entry and stay in Luxembourg under Luxembourg's new immigration law.[57] Before the bill entered into force, the CNPD issued an opinion on the article creating a new database, and allowing its officials direct access, for those purposes. In its opinion, the CNPD recommended that the Ministry specify the exact files to which it would have access, provide for retraceability of persons who accessed the database, and require that the files consulted have a direct relationship with the reason for which they were consulted.[58] The bill now includes those provisions.

[57] Luxembourg/*Loi du 29 août 2008 sur la libre circulation des personnes et l'immigration* [Law of 29 August on free movement and immigration] (29.08.2008), Art. 138.

[58] CNPD (2008) *Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal autorisant la mise en œuvre des traitements de données à caractère personnel nécessaires à l'exécution de la loi du … sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayent l'Immigration dans ses attributions peut accéder aux fins d'éffectuer les contrôles prévus par la loi, Délibération n° 202/2008 du 18 juillet 2008* [CNPD Opinion on draft Grand-Ducal Regulation on data processing for purposes of monitoring immigration law compliance, No. 202/2008of 18 July 2008].

2. Data Protection Authority

[51]. The CNPD's website has an English-language section that provides extensive information on the CNPD and its activities as well as an unofficial English translation of the 2002 Law that does not include the 2007 Law's amendments. Most of the legislative materials, reports, and opinions, however, are in French.[59]

[52]. Articles 32-37 of the 2002 Law provide for the CNPD, Luxembourg's DPA. The CNPD is an independent collegial body charged with monitoring that personal data are being processed according to the 2002 Law and its implementing regulations. It is a public authority established in the form of an *Etablissement Public* [Public Institution]. It has financial and administrative autonomy under the supervision of the Minister of Communications, and carries out its duties with complete independence. The CNPD is a collegiate body composed of three permanent members and three substitute members appointed and dismissed by the Grand Duke at the Cabinet's proposal. The Grand Duke appoints the CNPD president. The members are appointed for a six-year mandate which is renewable once. The Cabinet must propose at least one jurist and computer engineer with a completed university degree, as permanent member and substitute.[60]

[53]. Remuneration of the CNPD members is based on whether that member comes from the public or private sector. If the member comes from the public sector, he or she retains the salary and benefits associated with his or her public sector position. If the member comes from the private sector, his or her remuneration is calculated according to the applicable regime provide for State administration employees, but retains the social security coverage associated with his or her previous, private sector position. The CNPD president and permanent members receive a special indemnity, set by Grand-Ducal regulation, that takes into account the commitment required by the appointment to their positions.[61]

[54]. Members of the CNPD cannot be members of the Government, Chamber of Deputies, Council of State or the European Parliament. Nor can they carry out professional activities in a company or any other entity in the data processing field, or directly or indirectly hold

[59] http://www.cnpd.lu/en/index.html (12.15.2008).

[60] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34.

[61] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34(2).

an interest in such a company. A member of the CNPD's resignation occurs by operation of law once that member reaches 65 years of age.[62]

[55]. The CNPD presents an annual report to the Cabinet on its activities for a given year. The report serves to highlight the status of the notifications, prior authorisations, deficiencies or abuses that are not specifically covered by the applicable legal, administrative or regulatory provisions. The CNPD publishes its annual report on which the *Commission Consultative des Droits de l'Homme* (CCDH) [Consultative Commission on Human Rights].[63]

[56]. The CNPD's duties can be broken down into three basic components: supervision and publicising, advice and cooperation, and information and guidance. The supervision and publicising component consists mainly of the receipt, verification and registration of notifications given by the data controllers, as well as the activities associated with the implementation of data processing subject to prior authorisation. The advice and cooperation component consists of providing its opinion on all proposed legislative, administrative or regulatory measures concerning personal data processing, suggesting to the Government improvements or simplifications to proposed or existing measures, as well as approving data processing codes of conduct submitted to it by professional associations representing data controllers. The CNPD provides information and guidance, by advising the Government on the impact of evolving data processing technologies on the liberties and fundamental rights of individuals through studies, investigation and expert opinions, as well as promoting the public awareness of data subject rights and controller duties particularly as concerns data transfer to third countries.[64]

[57]. To the extent necessary for the accomplishment of their respective missions, the CNPD cooperates with its counterpart institutions in other EU Members States mainly by exchanging all pertinent

---

62 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34(2)-(4).

63 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(2).

64 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(3) and CNPD (2008) *The status and powers of Luxembourg's National Data Protection Commission (CNPD)*, p. 2, available at http://www.cnpd.lu/objets/publications/autres_publications/0508_status_powers.pdf (01.05.2009).

information. The CNPD represents Luxembourg in the Article 29 Data Protection Group.[65]

[58]. The CNPD's implementing regulations, published in the *Mémorial B* [Luxembourg's official administrative journal], cover the internal functioning of the CNPD, the rules of procedure before the CNPD and the services provided by the CNPD. The CNPD's hearings are not public. The CNPD's meetings and deliberations are valid only when three members are present. The CNPD is convened to deliberate either by its president or by two permanent members. No member can sit in, deliberate or take a decision concerning any matter in which he or she has a direct or indirect interest. Decisions are taken by a majority of votes and no abstentions are permitted. The Cabinet that nominated a member may also propose that member's dismissal to the Grand Duke. The CNPD's opinion on the proposed dismissal is heard before any dismissal is actually requested. The permanent and substitute members of the CNPD are not allowed to receive instructions from any authority when performing their duties.[66]

[59]. The State made a grant of initial funding of EUR 200,000 from the State budget when the CNPD was created. The State also provided the CNPD with its initial offices and office equipment. The CNPD has since moved and now pays its rent out of its budget. The 2002 Law authorises the CNPD to draw the funds necessary for compensation of its personnel and operating expenses from the fees it receives for notifications, notification amendments, prior authorisation requests and amendments to them. The expenses remaining would be covered by a grant of funds from the State budget, with the amount to be determined on an annual basis. The CNPD's separate budgetary line item is under the Ministry of State's media and communications subheading. In 2008 the CNPD received EUR 1,395,480 from the State budget and will receive EUR 1,476,000 in 2009.[67]

---

65 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34(9)-(10).

66 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 35 and Luxembourg/*Règlement intérieur adopté par la « Commission nationale pour la protection des données »*, Mémorial B no. 5 du 28 janvier 2003 (29.11.2002), pp. 124-129.

67 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 37, and Luxembourg/*Loi du 21 décembre 2007 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2008* (21.12.2007), p.4134, Luxembourg/*Loi du 19 décembre 2008 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2009* (19.12.2008), p.2820 and interview of 08.01.2009 with CNPD member.

[60]. The CNPD's staff currently consists of 9 paid employees. In addition to the three paid Commission members, the CNPD employs two jurists, two writers and two secretaries.[68]

[61]. The CNPD's powers include those to receive complaints and deal with cases. To that end, anyone, personally or through their lawyer or other physical or legal person duly appointed, can petition the CNPD to verify the legality of data processing as it relates to the respect of his or her liberties and fundamental rights. The CNPD will inform the data subject of the results of the request. In particular, data subjects may petition the CNPD to examine the legality of limitations on their right to access personal data. If any of the Labour Code entities mentioned above petition the CNPD, the CNPD must render a decision within one month of the petition.[69]

[62]. The CNPD's power to investigate claims gives it the power to access the data in question and collect all information necessary to perform its monitoring and verification tasks, including directly accessing the data on the premises on which it is processed, except when processed in a place of residence. The CNPD can bring a legal claim to enforce the 2002 Law and its implementing regulations, and it shall bring the infractions of which it becomes aware to the attention of law enforcement and legal authorities.[70]

[63]. Whosoever knowingly impedes or prevents the CNPD from carrying out its mission and duties shall incur sanctions of eight days' to one years' imprisonment and a fine ranging from EUR 251 to 125,000, or one of the two sanctions. Refusing to give access to the premises on which the data in question is being processed, provided the premises are not residential, is considered knowingly impeding the CNPD from carrying out its mission and subject to those sanctions. Likewise, refusing to provide all information and documents requested by the CNPD is subject to the same sanctions.[71]

[64]. The CNPD also has the power to impose the following administrative sanctions:

---

68 Telephone conversation of 13 January 2009 with member of the CNPD.

69 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(4)-(6).

70 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(7)-(9).

71 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(11).

1. warn or admonish the controller who has violated the provisions regarding subordination of data, safeguards, special safeguards and the obligation of confidentiality;

2. block, erase or destroy data under question in contravention of the 2002 Law or its implementing regulations;

3. temporarily or permanently prohibit data processing in contravention of the 2002 Law or its implementing regulations; and

4. order the publication in newspapers or under another format of an entire decision, or an extract thereof, prohibiting data processing, at the expense of the person sanctioned.

Application of the above sanctions can be appealed before the competent administrative tribunal.[72]

2.1. Article 28 Powers

[65]. The powers given to the CNPD correspond very closely to the requirements of Article 28 of Directive 95/46/EC. The CNPD acts with complete independence. As stated above, the 2002 Law provides that the CNPD has financial and administrative under the supervision of the Minister of Communications, and carries out its duties in complete independence.[73] Moreover, the CNPD is now routinely consulted when administrative or legislative measures are being prepared and adopted. The powers of the CNPD include the power to investigate that include the power to access the data the processing of which is in question, and the CNPD can directly access that data at the site of processing, provided that the processing site is not a residence.[74]

[66]. The CNPD has an effective power of intervention through its ability to require prior authorisation for certain data processing activities (more than simple prior checking) prior to the initiation of certain processing activities. The CNPD is also empowered to order the blocking, erasure or destruction of data, impose a temporary or definitive ban on

[72] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 33.

[73] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 34(1) and interview of 08.01.2009 with member of the CNPD.

[74] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(7) and interview of 08.01.2009 with member of the CNPD.

processing, to warn or admonish a controller or refer a matter to the appropriate authority. The CNPD's administrative sanctions mirror those in Article 28 of Directive 95/46/EC. The CNPD's powers to engage in legal proceedings cover proceedings in the enforcement of the 2002 Law and its implementing regulations, as well the obligation to bring to the attention of judicial authorities all infractions of which it becomes aware. Those powers also correspond almost *verbatim* with the Directive's requirements. Article 32(5) provides for the CNPD's power of investigation and intervention when the data subject's rights have been limited under the 2002 Law's exceptions to data access pursuant to Article 29.[75]

[67]. At this stage in its development, the CNPD's powers are sufficient to achieve effective data protection in Luxembourg. While one could argue that the purely administrative sanctions may not be a sufficient deterrent, the determination to have solely administrative sanctions was a legislative decision that the CNPD does not question. Monetary sanctions could lead to an abuse of power if the DPA were to pay its expenses with the sanctions it imposed. The same could be said for the obligation to pay an annual fee for a prior authorisation. In Luxembourg, fees for prior authorisations are payable only once unless there is an amendment to the authorisation.[76]

[68]. As stated above, the CNPD's remit mirrors that of the Directive and is sufficient for its purposes at this time. The imposition of monetary or criminal sanctions would be at the discretion of the competent tribunal. Given its short time in existence, the CNPD has concentrated on familiarising citizens with the legal requirements concerning data protection and promoting self-initiated compliance by the entities concerned, thus one could say that it has not fully explored the extent of its remit.[77]

[69]. At this time, the CNPD's budget is sufficient for it to carry out its mission and activities. That does not negate the possibility of requesting funding for additional personnel, particularly in positions of information technology expertise. At this time, the CNPD must subcontract outside information technology experts for the expertise at times required to carry out its investigations. In its first year of

[75] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 8, 14, 29, 32 and 33, and interview of 08.01.2009 with member of the CNPD.

[76] Interview of 08.01.2009 with member of the CNPD.

[77] Interview of 08.01.2009 with member of the CNPD; CNPD(2003*) Premier rapport au Gouvernemnt portant sur l'année 2002*, p. 4; and, CNPD (2004) *Rapport annuel* 2003, p. 16. *See also* CCDH (2005) *Avis de la CCDH sur le rapport annuel 2003 de la Commission Nationale pour la Protection des Données*, p. 1.

operation, the CNPD had 6 employees, so it focussed on monitoring data processing operations through formalities because it had few personnel and was unable to investigation activities. Now, the CNPD carries out several investigations and is working to complete them in a timely manner. Each time the CNPD has requested a funding increase, that increase has been accorded.[78]

[70]. The guarantee of independence granted to the CNPD is sufficient to ensure effective use of its powers. As stated above, the legislation creating the CNPD expressly provides for its independence. The only 'dependence' the CNPD has on the government is for its funding, but there is no governmental pressure to carry out its mission and duties in anything less than an independent manner. Moreover, a CNPD member's mandate is renewable only once and the CNPD's internal regulations contain specific provisions regarding the incompatibility of holding governmental, or other conflicting positions, with the CNPD member's mandate.[79]

[71]. At its creation in 2002, the CNPD was given sufficient powers to be a proactive institution, and is working toward that end. As mentioned above, the initial emphasis of the CNPD was to set up the formalities and procedures for compliance with Luxembourg's newly-created data protection regime. It was also necessary to allow Luxembourg's data controllers to adapt their policies and procedures to the 2002 Law. Now, the CNPD has begun to be proactive and carry out *grands audits* [big audits] on its own initiative. The purpose of these audits is to monitor compliance with the Data Retention Directive, and is carried out with the assistance of outside expertise in such entities as insurance companies, the social security administration and Luxembourg's labour inspectorate. Another area in which the CNPD is carrying out investigations on its own initiative is in the area of location data. The CNPD thoroughly investigates the increasing number of requests by employers for authorisation to use location data equipment.[80]

[72]. Given its short time in existence, the CNPD is still largely reactive with respect to data protection legislation compliance monitoring. Problems or a lack of compliance are mainly identified when the CNPD investigates the complaints that it receives. However, its website contains information on the privacy rights of data subjects and the data controller's responsibilities. In 2004, the CNPD put its first

[78] Interview of 08.01.2009 with member of the CNPD.

[79] Luxembourg/*Règlement intérieur adopté par la « Commission nationale pour la protection des données »*, Mémorial B no. 5 du 28 janvier 2003 (29.11.2002), Art. 9.

[80] Interview of 08.01.2009 with member of the CNPD, and CNPD (2008) *Rapport annuel* 2007, p. 22.

information brochure on its website. And, it participated in an informational campaign with the *Union Luxembourgeoise des Consommateurs* [Luxembourg Consumer's Union] whereby the two entities jointly published a data protection calendar.[81]

[73]. CNPD decisions and opinions are available on the CNPD's website and in the annual reports on its website. These include opinions on data processing concerning compliance with the immigration law, the interagency cooperation law, the free speech and judiciary and law enforcement data processing laws.[82]

[74]. While not considered binding, the opinions of the Working Party established under Article 29 of Directive 95/46/EC represent more than a source of inspiration for the CNPD's interpretation of Luxembourg's legislation implementing EU data protection legislation. Given that the CNPD is a member of the Article 29 Working Party, and participates in the creation of the opinions, it could be said that the Working Party's opinions represent the opinion of the CNPD itself.[83]

[75]. In its opinion authorising the Mondorf Spa finger print recognition system, the CNPD cites an Article 29 Working Party paper that describes a system similar to the one authorised, in which the data subject's recorded fingerprint data is accessible only by the data subject. It also cites to the Article 29 Working Party's WP 67 document on the principle of proportionality in its decision denying the operation of a videosurveillance system in a shoe repair shop located in a shopping centre.[84]

[76]. The CNPD's advisory role is much improved. Article 32(3) of the 2002 Law empowers the CNPD to render its opinion on proposed legislative measures, as well as to make suggestions to the government for the improvement of existing or proposed legislative measures in Luxembourg's data protection framework. When the CNPD was first created in 2002, the government did not routinely ask

---

81 Interview of 08.01.2009 with member of the CNPD. *See also* http://www.cnpd.lu/fr/.

82 Interview of 08.01.2009 with member of the CNPD. *See also* http://www.cnpd.lu/fr/.

83 Interview of 08.01.2009 with member of the CNPD.

84 CNPD (2006) *Déliberation no. 33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques* [Deliberation No. 33/2006 of 12 April 2006 of the CNPD on Domaine Thermal de Mondorf's prior authorization request for surveillance using biometric data], p. 10, and CNPD (2004), *Déliberation No. 1/2004 du janvier 2004 de la Commission nationale pour la protection des données relative aux demandes d'autorisation préalable en matière de vidéosurveillance de la société à responsabilité limitée*…, p. 16.

the CNPD for its opinion on proposed legislative measures on personal data protection. However, with the passing of time, and the CNPD's increasing role in Luxembourg data protection, the CNPD is now routinely asked by the Council of State to render an opinion on measures touching on data protection.[85]

[77]. The CNPD has been increasingly active in data protection awareness-raising in Luxembourg. It has created a brochure and website sections in French, English, German and Portuguese; held workshops and conferences to promote data protection awareness; and, is increasingly invited to conferences and schools to inform the public and young people on data protection. The data protection calendar that CNPD and Luxembourg Consumer's Union published jointly reached an estimated one-third of Luxembourg residents. On 28 January 2009, the CNPD will participate in International Data Protection Day. The CNPD continuously updates its websites with information, decisions, press releases and activities touching on data protection.[86]

[85] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 32(3), and interview of 08.01.2009 with member of the CNPD.

[86] Interview of 08.01.2009 with member of the CNPD. *See also* http://www.cnpd.lu/fr/.

3. Compliance

[78]. Luxembourg's data processing registration duties and duties for requesting approval of sensitive data processing operations in Luxembourg consist of the Directive's provisions regarding the contents of notification (controller's name and address, purpose of data processing, description of data categories, receivers of the data, contemplated third-country receivers, basic description of safeguards), In addition, Article 13 of the 2002 Law requires that the basis for the legitimacy of the processing be provided, and provides information on transmission and payment to the CNPD and as well as the simplified notification procedure.[87]

[79]. Article 14 of the 2002 Law requires prior authorisation, a more onerous procedure than simple prior checking, for data processing related to genetic data; recorded surveillance; historic, statistical or scientific purposes; data sharing; the credit and solvency of data subjects when performed by persons other than financial sector professionals or insurance companies for their clients; biometric data necessary to verify the identity of persons; and the use of data for purposes other than those for which it was collected, unless the data subject's prior consent has been obtained or it is necessary to save the data subject's vital interest. The article further specifies the information required in the authorisation request, the CNPD payment and transmission as well as simplified notification procedure information. Violation of Article 14 incurs sanctions of eight days to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[88]

[80]. In general the registration duties are complied with, but the CNPD cannot usually be aware of non-compliance unless a complaint is lodged. This applies particularly with respect to surveillance. Given the number of notifications/declarations the CNPD has to process and the simplified notification procedure, it is more difficult to detect if a notification has not been filed. It is usually easier to detect non-compliance with prior authorisation requirements, as that is a more visible violation of the requirement, particularly with respect to video

[87] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 13.

[88] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 14.

surveillance. Also, given that the sanctions the CNPD can impose are primarily administrative, there can at times be a compliance problem. In one instance, the CNPD denied authorisation for a videosurveillance system to a shoe repair business located in a shopping mall, but the company continued using the system. CNPD representatives had to visit the shop to ensure compliance with the decision denying the system.[89]

[81]. Article 40 of the 2002 Law covers the possibility for a controller to appoint a data protection officer, the powers of which are to investigate and monitor the controller's compliance with the 2002 Law and its implementing regulations. The data protection officer also has the right to receive information from the controller, and to inform the controller on matters of such compliance. The data protection officer is a natural or legal person who carries out his/her mission and activities independently of the controller. The data protection officer must be certified as such by the CNPD, and a Grand-Ducal Regulation further specifies the data protection officer's duties and activities.[90]

[82]. Under the Grand-Ducal Regulation, the data protection officer must provide proof of his or her competence in data processing on an annual basis to maintain the certification with the CNPD. Every four months, the data protection officer furnishes a listing of the data processing operations from his or her register. The CNPD maintains a public listing of its certified data protection officers.[91]

[83]. Before the 2002 Law was amended in 2007, there was no notification requirement to the CNPD of the controller's appointment of the data protection officer. After the 2007 amendment, the appointment of the data protection officer must be notified to the CNPD if that individual is external to the entity in question. An employee of that entity can also be appointed data protection officer, and in that case would not have to be notified to the CNPD. This is increasingly the case with compliance officers in banks. The appointment of an employee as a data protection officer promotes the data protection 'culture' in a company, and the CNPD assists that individual in learning about and carrying out his or her duties.[92]

---

89 Interview of 08.01.2009 with member of the CNPD.

90 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 40, and Luxembourg/*Règlement grand-ducal du 27 novembre 2004 concernant le chargé de la protection des données* (27.11.2004).

91 Luxembourg/ *Règlement grand-ducal du 27 novembre 2004 concernant le chargé de la protection des données* (27.11.2004), Arts. 1(2), 2 and 4. *See also* The Data Protection Officer, available at http://www.cnpd.lu/en/charge_protection/index.html (12.01.2009).

92 Interview of 08.01.2009 with member of the CNPD.

[84]. There is no evidence available indicating compliance or lack of compliance with data protection legislation in practice.[93]

[93] Interview of 08.01.2009 with member of the CNPD. Also, the State Prosecutor's office responded to our letter of 5 December 2008, requesting statistics with two 2008 judicial decisions.

4. Sanctions, Compensation and Legal Consequences

[85]. Pursuant to Article 33 of the 2002 Law, the CNPD is empowered to impose administrative sanctions only. At this time the CNPD considers the sanctions to be sufficient, particularly given that courts have the discretion to impose criminal sanctions and fines. Given the relatively short existence of the CNPD, one can only begin to count the application of its sanctions from 2003 onward. In 2003 and 2004, the CNPD imposed no sanctions. In 2005, the CNPD imposed one sanction data processing ban. Similarly, in 2006, the CNPD imposed one data processing ban. And, in 2007, Luxembourg District Court's Criminal Court imposed a fine of 5,000 EUR.[94]

[86]. At this time the State Prosecutor's Office has not responded to our request for statistics on sanctions and/or compensation payments, and the range of sanctions and/or compensation payments in cases regarding personal data processing.[95]

[87]. Many of the sanction provisions in the 2002 Law provide for the imposition of sanctions when one knowingly (*sciemment*) violates the provisions in question only with respect to the data subject's right to access to his or her personal data, the patient's right to his or her personal data information, the data subject's right to object and anyone's impeding or preventing the CNPD's carrying out of its mission. Otherwise, the 2002 Law simply provides for the imposition of sanctions when one violates its provisions.[96] Similarly, the 2005 Law provides the sanctions when one violates its provisions.[97]

[88]. Negligence is not discussed in the law or in the jurisprudence.

---

94 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 33, and telephone conversation of 13.01.2009 with member of the CNPD.

95 Letter of 5 December 2008 to State Prosecutor's Office.

96 Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Arts. 28((2) and (7), 30(2) and 32(11).

97 Luxembourg/*Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard tu traitement des données à caractère personnel dans le secteur des communications électroniques, etc.* (30.05.2005).

[89]. As stated above, at this stage in the CNPD's work, problems are mostly identified when the CNPD investigates the complaints it receives. However, at times the Luxembourg Consumer's Union (through its member businesses) and the labour inspectorate refer cases to the CNPD. These cases deal mostly with surveillance. In turn, the CNPD must refer violations of which it becomes aware to the State Prosecutor's Office. The CNPD's follow-up activities consist mainly of monitoring compliance with its decisions. Depending on the type of data processing, the CNPD may have to visit the premises of the data processing. At this time the follow-up activities do not usually lead to sanctions and/or compensation payments in Luxembourg because the entity being monitored usually complies with the CNPD's decisions, and if they do not, it is often due to a lack of knowledge of the legal requirements.[98]

[90]. At this time, enforcement of data protection legislation through sanctions and/or compensation payments in Luxembourg depends largely on the personal initiative, and complaints, of data subjects. Data subjects are informed of their rights by the CNPD, the CNPD's extensive website, and the Luxembourg Consumer's Union. The financial burden of legal procedures regarding data protection in Luxembourg are borne by the State only in criminal cases, otherwise the financial burden is shared by the parties. To date, however, there have not been many data protection cases in Luxembourg.[99]

[91]. The provisions regarding processing for surveillance in the workplace originally in the 2002 Law are now found in the Luxembourg Labour Code that was promulgated in 2006. If the employer is the controller, data processing for purposes of surveillance at the workplace can only be carried out under the conditions set forth in the Luxembourg Labour Code requiring that the surveillance be carried out with the prior approval of the CNPD, and that the processing be necessary for:

(1) workers' security and health needs;

(2) the company's property protection needs;

(3) inspection of the production process solely relating to machines;

(4) temporary inspection of the worker's labour/services provided, when such inspection is the only way of determining the exact remuneration; or

[98] Interview of 08.01.2009, and telephone conversation of 13.01.2009 with member of the CNPD.

[99] Interview of 08.01.2009 with member of the CNPD.

(5) in the context of organisation of flextime under the Luxembourg Labour Code.

[92]. For numbers 1, 4 and 5 above, the company joint committee, to be set up if necessary, has the power to decide on (1) the introduction or application of technical facilities that would inspect the worker's behaviour and performance on the job, and (2) the introduction and amendment of measures regarding workers' health and security as well as the prevention or workplace illnesses. The data subject's consent does not legitimate the employer's processing of the data. Without prejudice to the data subject's right to information, the employer must give prior notice to the data subject, and for persons falling under the private law contract regime, the joint committee, or if none, the personnel delegation, or if none, *l'Inspection du travail et des mines* [Luxembourg's labour inspectorate]. For persons falling under the statutory regime the employer must give prior notice to the data subject and the bodies representing personnel as provided by the applicable laws and regulations. A violation of these Luxembourg Labour Code provisions is subject to the same sanctions as those for Article 10.[100]

[100] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 11; Luxembourg/*Code du Travail* (01.10.2008), Art. L. 261-1, L.261-2 and L.423-1.

5. Rights Awareness

[93]. There are no other studies and surveys on awareness regarding data protection law and rights in the Luxembourg other than the two 2008 Eurobarometer surveys.[101]

[94]. The 2008 Eurobarometer Study regarding citizens' perceptions of data protection in Luxembourg revealed that among the organisations that may hold personal data on an individual, the 1000 citizens interviewed most trusted the social security administration (87.7%) and medical services and doctors (83.8%). Other organisations such as tax and local authorities (both at 80.4%); police (79.3); and banks, financial authorities (78.7) also had a relatively high percentage of trust among Luxembourg citizens, as compared to mail order and travel companies that had the lowest percent of trust (24.9% and 52.1%, respectively). Credit card companies and employers benefited from a relatively high level of trust (67.5% and 66%, respectively). Credit reference agencies, market opinion and research companies, and non-profit organisations had a relatively low level of trust (48.5%, 47.7% and 41.5%, respectively).[102]

[95]. Interestingly, while of the 1000 persons surveyed only 28.7% had heard of the existence of Luxembourg's CNPD (compared to the EU27 average of 28.2%), a high percentage (20.6%) had contacted that institution as compared to the EU27 average of 6.2%. And, as a general matter, concern among Luxembourg citizens concerned about data privacy by organisations that hold personal data increased by about 5% between 1991-2008 (from 61% to 65%), while those who were unconcerned remained stable (from 31% to 30%) over that same time period.[103]

[96]. These findings indicate that the best areas for the CNPD and Luxembourg's data protection framework to target its effort remain sensitising the public about its own existence and Luxembourg's data protection framework. They also indicate that while the CNPD may not be as widely known as one might wish, those citizens who are aware of its existence are quite comfortable with contacting that institution.

---

[101] Interview of 08.01.2009 with member of the CNPD.

[102] European Commission (2008) *Flash Eurobarometer, Data Protection in the European Union, Citizens' perceptions, Analytical Report*, at pp. 74-75.

[103] European Commission (2008) *Flash Eurobarometer, Data Protection in the European Union, Citizens' perceptions, Analytical Report*, at pp. 104, 110 and 8.

[97]. According to the 2008 Eurobarometer Study regarding data controllers' perceptions of data protection in Luxembourg, 50% felt that the requirements of the data protection law were 'somehow too strict'. And, Luxembourg was the only EU Member State in which more than half of the respondents (55%) would agree that, with the exception of certain sectors, the requirements of the data protection law were unnecessary. The respondents also deemed that the luxembourg data protection law was more rigorously applied and interpreted than in other EU Member States. Of the 106 data controllers and enterprises surveyed, a large majority (86.4) rather agreed, however, that the requirements of the data protection law were necessary to protect consumers' rights and the fundamental rights of citizens. And, 5.4% of the companies had received complaints from persons whose data was being processed, more than double the EU27 average of 2.6%. However, 15.3% were in regular contact with the CNPD, as compared to the EU27 average of 12.6%.[104]

[98]. These findings could indicate that the legislation itself may continue to undergo amendments in the direction of simplification. Nonetheless, given the short existence of the CNPD, the figures indicate that its contact with controllers and companies is positive and relatively widespread.

[104] European Commission (2008) *Flash Eurobarometer, Data Protection in the European Union, Data controllers' perceptions, Analytical Report*, at pp. 17, 19, 22, 63, 89 and 95.

6. Analysis of deficiencies

[99]. During its short time in existence, the CNPD has concentrated its efforts on informing the relevant parties of their rights and responsibilities. One cannot be well-equipped to comply with one's duties or assert one's rights without being well informed. Major deficiencies in Luxembourg's data protection regime may appear in time, but at this point there are no major deficiencies.[105]

[100]. Areas not covered by the 2002 Law are the exceptions carved out in the 2002 Law's Article 17, which lists the areas governed by Grand-Ducal Regulation. The regulations cover general processing necessary for law enforcement agencies such as the Grand-Ducal Police, and the disciplinary bodies of the police and customs and duties administration. They also cover processing related to State security, defence, public security, as well as that involved in criminal law investigation under international accords, intergovernmental agreements or Interpol. Moreover, the use of closed-circuit television in high-risk public areas for protection and law enforcement purposes is governed by Grand-Ducal regulation.[106]

[101]. Monitoring of data processing under national or international law is performed by an authority composed of the State Prosecutor, or an appointed delegate in the matter, and two members of the CNPD that the Minister of Communications names at the suggestion of the CNPD. The CNPD's organisation and functioning are regulated by Grand-Ducal regulation. The CNPD can directly access all data that is the subject of any dispute or about which it performs an investigation. A violation of Article 17 in the private sphere incurs sanctions of eight days' to one year's imprisonment and a fine ranging from EUR 251 to 125,000, or either one of the two sanctions. The tribunal asked to adjudicate a matter can order that the data processing be stopped under penalty of a fine the maximum of which the tribunal itself has the discretion to set.[107]

[102]. Further exempt processing is that carried out by lawyers, notaries and bailiffs when related to legal defence; that carried out for purposes of journalism or literary or artistic expression; and that necessary to save the vital interests of the data subject or another person when the data

[105] Interview of 08.01.2009 with member of the CNPD.

[106] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 17(1).

[107] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (02.08.2002), Art. 17(2)-(3).

subject is physically or legally incapable of giving his or her consent is not subject to the notification requirement.[108]

Paragraph 31 above lists the 14 exceptions to the notification requirement for personal data processing carved out by Article 12 of the 2002 Law.[109]

[103]. At this time, the CNPD and Luxembourg are still stabilising the personal data protection framework and deem that over time increased resource allocation, awareness raising and training will reveal the deficiencies that must be addressed. Moreover, the CNPD is sufficiently empowered to suggest remedial measures to the government or other entities.[110]

[108] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Art. 12(1)-(2).

[109] Luxembourg/*Loi du 2 août 2002 relative à la protection des personnes à l'égard tu traitement des données à caractère personnel* (02.08.2002), Artt. 12(3)-(4).

[110] Interview of 08.01.2009 with member of the CNPD.

7. Good practices

[104]. One example of a good practice is the CNPD's decision in the Mondorf case in which the CNPD authorized Mondorf Thermal Spa's second request for authorisation of a member biometric data recording/surveillance system (fingerprints), after denying a prior request (see also Annex 2c – Case Law). The original request was for authorization of an already operative system that would record and store fingerprint data in a central database. Members had complained to the CNPD about the system in operation. The CNPD banned use of that system on 12 December 2005. The second request proposed a system that would store the recorded data on member bracelet chips, to which only that member would have access. The case was heavily covered by the media and involved the CNPD's use of its administrative sanction powers by banning the system in operation, but allowed the spa to propose an alternative system that was ultimately authorized. On page 10 of its 2006 decision authorizing the system, the CNPD cites to an Article 29 Working Party paper recommending a system such as the one ultimately authorized, whereby only the data subject has access to the recorded data, as being one that poses the least threats to fundamental rights. [111]

[105]. In general, the CNPD's multilingual website materials are quite extensive and provide a wealth of information to Luxembourg data subjects, controllers, processors and lawmakers.[112]

[111] CNPD (2006) *Déliberation no. 33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques* [Deliberation No. 33/2006 of 12 April 2006 of the CNPD on Domaine Thermal de Mondorf's prior authorization request for surveillance using biometric data], and Interview of 08.01.2009 with member of the CNPD.

[112] http://www.cnpd.lu/fr/.

8. Miscellaneous

[106]. In December of 2008, the Law on cooperation between fiscal administrations was passed into law. The law provides for the exchange of information among tax administrations; the exchange of data among the customs, one tax administration and the labour inspectorate; and, the exchange of data between the two tax administrations and many of the social security funds and ministry of transport. The stated purpose of the law is to ensure recovery of tax payments, fight tax fraud and guarantee equality of citizens and companies with regard to taxation.[113]

[107]. In its advisory opinion on the proposed bill, the CNPD noted that while the bill did not contain the words 'data interface', even though the bill's main purpose was to ensure just that. Also, the CNPD expressed the concern that no criteria for safeguards were specified in the bill.[114] The text voted into law contains the wording that the data interface will take place under guaranteed conditions of secured, limited and controlled access.[115]

[113] Luxembourg/*Loi du 19 décembre 2008 ayant pour objet la cooperation interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions Directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises* (19.12.2008).

[114] CNPD (2007) Avis de la Commission nationale pour la protection des données concernant l'avant-projet de loi ayant pour objet *la cooperation interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions Directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises.*

[115] Luxembourg/*Loi du 19 décembre 2008 ayant pour objet la cooperation interadministrative et judiciaire et le renforcement des moyens de l'Administration des Contributions Directes, de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises* (19.12.2008) Arts. 1, 4, 7, 11(3), 12 and 13.

Annexes

Annex 1 – Tables and Statistics[116]

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	Not yet established	Not yet established	Not yet established	500,000 EUR[117]	900,000 EUR[118]	978,000 EUR[119]	1,028,100 EUR[120]	1,029,000EUR[121]
Staff of data protection authority				Total: 6 3 members	Total: 8 3 members	Total: 8 3 members	Total: 8 3 members	Total: 9 3 members

[116] All statistics, except for the budgetary figures, were provided during a telephone conversation of 13.01.2009 with a member of the CNPD. The State Prosecutor's office responded to our letter of 5 December 2008, requesting statistics with two 2008 judicial decisions.
[117] Luxembourg/*Loi du 20 décembre 2002 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2003* (20.12.2002), at p. 3284.
[118] Luxembourg/*Loi du 19 décembre 2003 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2004* (19.12.2003), at p. 3738.
[119] Luxembourg/*Loi du 21 décembre 2004 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2005* (21.12.2004), at p. 3026.
[120] Luxembourg/*Loi du 23 décembre 2005 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2006* (23.12.2005), at p. 3441.
[121] Luxembourg/*Loi du 22 décembre 2006 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2007* (22.12.2006), at p. 4370.

				2 functionary writers 1 secretary	2 functionary writers 2 secretaries 1 jurist	2 functionary writers 2 secretaries 1 jurist	2 functionary writers 2 secretaries 1 jurist	2 functionary writers 2 secretaries 2 jurists

Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative				0	2	3	5	7
Number of data protection registrations				4,879	2,170	1,554	1,454	1,840
Number of data protection approval procedures				1,483	420	334	314	543
Number of complaints received by data protection authority				15	38	40	30	34
Number of complaints upheld by data protection authority				10	30	31	23	27

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)				10*	30*	31*	23*	27*
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)				0	0	CNPD: 1 data processing ban	CNPD:1 data processing ban	District Criminal Court: 1 fine of 5,000 EUR
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)				No statistics available	No statistics available	No statistics available	No statistics available	5,000 EUR

*Unable to disaggregate figures, each complaint was accorded follow up.

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2a – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	*Appeal by XY Company Luxembourg, Sàrl against decision by the CNPD*
Decision date	31.01.2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Numéro de rôle 19234C, Cour Administrative du Grand-Duché de Luxembourg* [Docket No. 19234 C, Grand Duchy of Luxembourg Administrative Court]
Key facts of the case (max. 500 chars)	The company, a shoe repair/key store located in a shopping centre, appealed a 9 January 2004 CNPD decision not authorising the company's on-site videosurveillance camera. The company sent the CNPD two authorisation requests; one based on Article 11 (processing for workplace surveillance purposes, given the risk to the security and health of workers, and the security of the company's goods posed by the workers), and one based on Article 10 (processing for surveillance purposes, given the risks posed to its goods by customers and third parties, and the risks to the safety of users).
Main reasoning/argumentation (max. 500 chars)	The Administrative Court upheld the lower Administrative Tribunal's confirmation of the CNPD's decision/ analysis of the 2002 Law's principles of interpretation, finding the necessity requirement unmet because the processing was not necessary given the minimal risks posed. The proportionality requirement was unmet because the proposed surveillance appeared to be more to supervise the workers themselves rather than the store's goods, and was an invasion of the workers' privacy, whereas Article 11 required that workers' health and safety be the aim of workplace surveillance.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Workplace surveillance must privilege workers' safety; necessity means there are no less intrusive means available; proportionality means the ends must justify the means of the surveillance and the infringement of privacy rights the surveillance entails.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The appellant company was ordered to pay the fees and expenses for the appellate proceedings. An employer cannot have an on-site videosurveillance camera if there are no legitimate threats to worker, customer or third-party safety.
Proposal of key words for data base	Videosurveillance; workplace surveillance; necessity; proportionality;

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Annex 2b – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	*X v. Company Y Luxembourg S.A.*
Decision date	26.01.2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Numéro de rôle 29384, La Cour d'appel du Grand-Duché de Luxembourg* [Docket No. 29384, Grand Duchy of Luxembourg Court of Appeals]
Key facts of the case (max. 500 chars)	Appellant requests the Court to rule his dismissal improper. After giving prior notice, Company Y fired appellant for having routinely not complied with his flextime working hour requirements, and having knowingly falsified time sheets by indicating hours worked when not at work. Appellant argued that the flextime tracking system recording entry and exit of employees through badge scanning and its report (gate audit) were inaccurate and that Company Y needed CNPD authorisation and a favourable mixed labour committee decision to have legally installed the system.
Main reasoning/argumentation (max. 500 chars)	The Court ruled the dismissal proper because appellant did not qualify as illegal the employer's evidence (gate audit, work hours recorded, time sheets), but argued that the hours recorded were inaccurate. Appellant did not provide days/times not showing on gate audit when he was at work, or deny having flextime, so that he should be aware/willing that employer would use such a system to monitor compliance with his 40-hour weekly contractual obligation. The employer's effort to periodically monitor compliance did not negate the value of the evidence. No need for 2002 Law analysis.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Under these facts, Company Y's possible irregularity regarding data protection legislation does not compromise his right to a fair proceeding, or damage the reliability of the evidence disputed by the parties, particularly when appellant did not move to have any of his employer's evidence excluded. An employer's occasional use of an hour control monitoring mechanism for flextime employees does not render the data unusable for legal evidentiary purposes.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Appellant's request for compensation for proceeding costs denied, he was required to pay all fees and expenses involved in appeal. Company Y's request for compensation for proceeding costs also denied. Company Y was required to pay sums not included in appeal expenses.
Proposal of key words for data base	Flextime administration/monitoring, badge scanning system, personal data and employment surveillance

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Annex 2c – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	*Déliberation no. 33/2006 du 12 avril 2006 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques* [Deliberation No. 33/2006 of 12 April 2006 of the CNPD on Domaine Thermal de Mondorf's prior authorisation request for surveillance using biometric data]
Decision date	12.04.2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Déliberation no. 33/2006, Commission nationale pour la protection des donnée* [Deliberation No. 33/2006, CNPD]
Key facts of the case (max. 500 chars)	CNPD authorized Mondorf Thermal Spa's second request for authorisation of a member biometric data recording/surveillance system (fingerprints), after denying a prior request. The original request was for authorisation of an already operative system that would record and store fingerprint data in a central database. Members had complained to the CNPD about the system in operation. The CNPD banned use of that system on 12 December 2005. The second request proposed a system that would store the recorded data on member bracelet chips, to which only that member would have access.
Main reasoning/argumentation (max. 500 chars)	Under Article 10 (processing - surveillance purposes) analysis, CNPD rejected the first application because databases accessible by other than members, possible use for other than intended surveillance. CNPD authorised the second request because that system allowed access to recorded personal data only by the member on the condition that: data not stored in central databases; an explanatory brochure be given data subjects prior to/at

	membership; all biometric data erased/returned to data subject at membership termination; and, data fairly processed/used for authorised purposes.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Processing for surveillance under Article 10 of the 2002 Law requires informed consent (brochures required by second authorisation). Given that biometric data is particularly susceptible to use for unintended purposes and the technology collecting biometric data is not completely controlled/controllable at this stage of its development, more data than is necessary should not be accessible by other than the data subject. Finger print data reveals the identity of the individual and thus requires special safeguards.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	After the first CNPD decision, the CNPD imposed a ban on use of the system (administrative sanction), and denied the authorisation. The second decision resulted in the CNPD's authorisation of the system.
Proposal of key words for data base	Data protection, biometric data, fingerprint data, informed consent

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Annex 2d – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	*Public Prosecutor v. X*
Decision date	28.02.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Arrêt No. 126/07X, La Cour d'appel du Grand-Duché de Luxembourg, dixième chambre, siégeant en matière correctionnelle* [Order No. 126/07X, Grand Duchy of Luxembourg Court of Appeals, 10th Chamber, Criminal Matters]
Key facts of the case (max. 500 chars)	A Luxembourg Post and Telecommunications (PTT) surveillance camera in a 'sensitive area' filmed an individual in '*flagrant délit*' and a prosecution was initiated based on two video tapes as sole evidence. The PTT did not have CNPD's prior authorisation, the request for which was pending before the CNPD since the year before the crime. The defence requested the evidence not be admitted because it was gathered in violation of Article 14 (prior authorisation) of the 2002 Law. The Public Prosecutor argued that the 2002 Law did not prohibit use of illicitly gathered information as evidence in legal proceedings.
Main reasoning/argumentation (max. 500 chars)	After surveying BE, FR and Swiss jurisprudence to contrary, Court of Appeals upheld District Court's ruling that evidence inadmissible, and dismissed case. Evidence can be freely introduced in Luxembourg criminal cases when it does not prevent a fair trial. No text explains procedure to exclude illicit acts (illegally gathered evidence) from a *preliminary* investigation. One's video image is sensitive data to be treated carefully; severity of a crime and its penalty must be balanced against degree to which information was illicitly gathered, particularly when sole evidence.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Illicitly gained evidence submitted by Public Prosecutor in criminal case not admissible when sole evidence for conviction. Illicit installation of video camera and recording of video image without prior authorisation punishable under 2002 Law.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Destruction of videotapes ordered, State to pay legal fees and costs.
Proposal of key words for data base	Right to information, videosurveillance, sufficiency of evidence

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Annex 2e – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	Appeal by Company … S.A. against the CNPD's decision on videosurveillance
Decision date	21.05.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Numéro du rôle 23155C Cour Administrative du Grand-Duché de Luxembourg* [Docket No. 23155C Grand Duchy of Luxembourg Administrative Court] and *Numéro du rôle 22050, Tribunal administratif du Grand-Duché de Luxembourg* [Docket No. 22050, Grand Duchy of Luxembourg Administrative Tribunal]
Key facts of the case (max. 500 chars)	A large grocery store in a shopping center appealed portion of CNPD's decision denying its request to use surveillance cameras in its questioning rooms on the grounds that no legal provision allows the a supermarket to film and record interrogation of presumed shoplifters. The store argued that filming of images and transmittal of sound was necessary for the safety of security personnel questioning individuals caught stealing merchandise, and would only be used for the purposes of the questioning sessions.
Main reasoning/argumentation (max. 500 chars)	Because appellant did not timely notify other parties to earlier proceeding of its appeal, the Administrative Court dismissed the appeal of the Administrative Tribunal's confirmation of the CNPD's decision that the store failed to show that surveillance could not be carried out by other means and that no other measures could ensure the security personnel's safety. Thus, intrusiveness represented by the filming and recording of personal data not proportional to necessity. Also, appellants did not provide evidence of prior attacks by presumed shoplifters on security personnel.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Degree of necessity required for videosurveillance in supermarket interrogation rooms.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Company was ordered to pay legal fees and costs incurred in the appeal.
Proposal of key words for data base	Videosurveillance, interrogation

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).