ORIGINAL

HinckleyAllenSnyderLLP
ATTORNEYS AT LAW

28 State Street
Boston, MA 02109-1775
TEL: 617.345.9000
FAX: 617.345.9020
www.haslaw.com

Laura B. Angelini
langelini@haslaw.com

December 24, 2008

VIA ELECTRONIC MAIL AND FIRST CLASS MAIL

Donald S. Clark
Secretary of the Federal Trade Commission
600 Pennsylvania Avenue, NW, Room H-135
Washington, DC 20580

RE: In the Matter of Polypore International, Inc., Case No. 9327

Dear Mr. Clark:

Enclosed please find courtesy copies of various articles and other authorities referenced in The Moore Company's Memorandum of Law in Support of Motion to Limit Subpoena *Duces Tecum* and for Cost Reimbursement.

If you have any questions regarding the enclosed, please call me.

Sincerely,

Laura B. Angelini

LBA/cz
Enclosures

cc:
Eric D. Welsh, Esq. (w/encl. - via e-mail)
Michael J. Connolly, Esq.

31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or

communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person

to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important

public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or

financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their

legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in

performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations

which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and

rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF

INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities

which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of

20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.

Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by

the Law of 31 July 2006
the Law of 22 December 2006
the Law of 27 July 2007.

Chapter I. General provisions relating to the protection of the person with regard to the processing of personal data

Article 1. Purpose

(Law of 27 July 2007)

"This law protects the fundamental rights and freedoms of natural persons, particularly their private lives, as regards the processing of personal data (...)."

Article 2. Definitions

For the purposes of this Law:

(a) "*code of conduct*": sector contributions drawn up in order to apply this Law correctly. Codes of conduct are drawn up at a national or community level by professional associations and other organisations representing the controllers, and may optionally be submitted to the Commission Nationale or the group for the protection of individuals with regard to the processing of personal data, as provided under Article 29 of Directive 95/46/EC;

(b) *"Commission Nationale"*: the Commission Nationale pour la Protection des Données [National Commission for Data Protection];

(Law of 27 July 2007)

"(c) *"consent of the data subject"*: any (...) free, specific and informed indication of his wishes by which the data subject or his legal, judicial or statutory representative signifies his agreement that the personal data may be processed;"

(d) *"recipient"*: will mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; authorities which may receive personal data pursuant to the performance of a legal or supervisory inquiry or task will not be regarded as recipients;

(Law of 27 July 2007)

"(e) *"personal data"* (hereinafter referred to as "data"): any information of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person ('data subject'); a natural (...) person will be considered to be identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, genetic, mental, cultural, social or economic, identity;"

(f) "*health data*" any information about the data subject's physical or mental state, including genetic information;

(g) *"genetic data"*: any data concerning the hereditary characteristics of an individual or group of related individuals;

(e) *"personal data filing system"* (hereinafter referred to as "filing system"): will mean any structured set of data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(i) "*medical authority*": any health practitioner and any person subject to the same professional secrecy obligation as well as any hospital covered by the Law of 28 August 1998 on hospitals, carrying out the data processing necessary for the purpose of preventative medicine, medical diagnosis, provision of care or treatment, or health service management;

"combination": abolished by the Law of 27 July 2007

(j) *"Minister"*: the Minister in charge of data protection;

(Law of 22 December 2006)

(k) "*social security body*": any public or private body that provides optional or compulsory services relating to sickness, maternity, old age, physical accident, invalidity, dependency, death, unemployment, "parental leave" as well as any family benefits or social assistance;

(l) "*third country*": non-Member State of the European Union;

(Law of 27 July 2007)

"(m) *"data subject"*: any natural (...) person who is the subject of data processing of a personal nature;"

(n) *"controller"*: a natural or legal person, public authority, agency or any other body which solely or jointly with others determines the purposes and methods of processing personal data. When the purposes and methods of processing are determined by or pursuant to legal provisions, the controller is determined by or pursuant to specific criteria in accordance with those legal provisions;

(o) "*processor*": a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(Law of 27 July 2007)

"(p) *"supervision"*: any activity which, carried out using technical instruments, consists of observing, collecting or recording in a non-occasional manner the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised instruments;"

(q) *"third party"*: any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data. In the public sector, a third party means a ministry, Civil Service department, public institution, regional authority or public service other than the controller or his processor;

(r) *"processing of personal data" (hereinafter referred to as "processing"):* any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Article 3 – Scope

(Law of 27 July 2007)

"(1) This Law will apply to:

- the processing of data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system;

- to any form of capture, processing and dissemination of sounds and images allowing that identify natural persons;

- the processing of data relating to public security, defence, seeking out and prosecuting criminal offences, or the State security, even if those data are related to a major economic or financial interest of the State, without prejudice to the specific provisions of national or international law governing these areas.

(2) The following is governed by this Law:

(a) processing by a controller established on the territory of the Grand Duchy of Luxembourg;

(b) processing by a controller who is not based on Luxembourg territory or the territory of any other Member State of the European Union but uses processing resources situated on Luxembourg territory, apart from resources that are used only for the purposes of transit through the said territory or that of another European Union Member State.

As regards the processing stated under Article 3, paragraph (2) letter (b), the controller will appoint by written declaration to the Commission Nationale a representative based on Luxembourg territory who will take the controller's place in fulfilling his obligations as stated under this Law without releasing the latter from his own liability.

(3) This Law will not apply to processing carried out by a natural person pursuant exclusively to his personal or

domestic activities."

Chapter II. Conditions governing the lawfulness of processing

Article 4. Data quality

(1) The controller will ensure that he processes the data in a fair and lawful manner, and notably that the data are:

(a) collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes.

(b) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(c) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(d) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed without prejudice to paragraph (2) below.

(Law of 27 July 2007)

"(2) The subsequent processing of data for historical, statistical or scientific purposes is not deemed incompatible with the purposes specified for which the data was collected."

(3) Any party who carries out processing in breach of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 5. Legitimacy of processing

(Law of 27 July 2007)

"(1) Data may be processed only (...):

(a) if it (...) is necessary for compliance with a legal obligation to which the controller is subject; or

(b) if it (...) is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(c) if it (...) is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(d) if it (...) is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1, or

(e) if it (...) is necessary in order to protect the vital interests of the data subject; or

(f) if the data subject has given his consent."

(2) Any party who carries out processing in breach of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 6. Processing of specific categories of data

(1) Processing operations that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life, including the processing of genetic data, are forbidden.

(2) Paragraph (1) will not apply where:

(Law of 27 July 2007)

(a) the data subject gave his "express" consent to such processing, subject to the inalienability of the human body and unless forbidden by law, or where

(Law of 27 July 2007)

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller (...) in the field of employment law in so far as it is authorised by law, or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out with the consent of the data subject by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim in the course of its legitimate activities and on condition that the processing relates to the necessary data solely of members of that body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to third parties without the consent of the data subjects; or if

(e) the processing relates to data that have been clearly made public by the data subject, or

(Law of 27 July 2007)

"(f) the processing (...) is necessary to acknowledge, exercise or defend a right at law (...), or if

(g) the processing is necessary in the public interest for historical, statistical or scientific reasons without prejudice to Article 7 hereafter (...), or if

(h) the processing is implemented via a Luxembourg regulation as stated in Article 17, or if"

(Law of 27 July 2007)

"(i) the processing is implemented in the context of the processing of legal data within the meaning of Article 8."

(...)

(3) Nevertheless, (...) genetic data may be processed only:

(a) to verify the existence of a genetic link for the purpose of legal proof, for compensation of the data subject, or the prevention or punishment of a specific criminal offence in the cases covered by paragraph (2) letters (f), (h) and (i) of this Article, or

(b) in the case covered by paragraph (2) letter (c) of this Article if the processing is necessary to protect the vital interests, or

(c) in the case covered by paragraph (2) letter (g) of this Article if the processing is necessary in the public interest for historical, statistical or scientific reasons, or

(d) in the case covered by Article 7, paragraph (2) of this Law if the data subject has given his consent and if the processing is carried out only in the area of healthcare or scientific research subject to the inalienability of the human body and except where the law provides that the prohibition stated in paragraph (1) cannot not lifted by the data subject's consent.

In cases where the law allows the prohibition to be lifted by the data subject's consent but for practical reasons it proves to be impossible to obtain consent or disproportionate to the objective sought and without prejudice to the right of opposition on the part of the data subject, the requirement to obtain prior consent may be overridden, subject to conditions to be laid down in a Luxembourg regulation, or

(e) in the case covered by Article 7, paragraph (1) of this Law if the processing of genetic data is necessary for the purpose of preventive medicine, medical diagnosis or the provision of care or treatment. In this case the processing of this data may only be carried out by the medical authorities."

(4) Any party who carries out a processing operation or notifies a third party in violation of the provisions of the aforementioned paragraph (1) is liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties. The court hearing the case may order the discontinuance of processing or communication that are contrary to the provisions of paragraph 1 of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 7. Processing of specific categories of data by the health services

(Law of 27 July 2007)

"Without prejudice to application of Article 6, paragraph (3) concerning the processing of genetic data:

(1) The processing of data on health and sex life necessary for the purpose of preventative medicine, medical diagnosis or the provision of care or treatment may be carried out by the medical authorities.

(2) The processing of data on health and sex life necessary for the purpose of healthcare or scientific research may be carried out by the medical authorities, or by the research bodies or the natural or legal persons whose research project has been approved under the legislation applicable to biomedical research. If the controller is a legal entity, it shall indicate a delegated controller, who shall be subject to

professional secrecy.

(3) The processing of data on health and sex life necessary for the management of healthcare services may be carried out by the medical authorities or, if the controller is subject to professional secrecy, by social security bodies and authorities that manage the said data in performance of their legal and regulatory tasks, by insurance companies, pension fund management companies, the *Caisse Médico-Chirurgicale Mutualiste* and by those natural or legal persons authorised to do so for socio-medical or therapeutic reasons under the Law of 8 September 1998 governing relations between the State and the bodies working in the areas of social security, family and therapeutic matters where their activity falls with the areas to be listed in a Luxembourg regulation.

(4) The processing may be sub-contracted subject to the conditions laid down in Article 21.

Provided their processing is in itself lawful as stated in Articles 6 and 7, the data covered therein may be notified to third parties or used for research purposes in accordance with terms and subject to conditions to be determined by Luxembourg regulations.

The providers of care and suppliers may communicate the data concerning their services to the general practitioner and to a social security body or to the *Caisse Médico-Chirurgicale Mutualiste* for the purpose of repayment of the corresponding expenditure.

(5) Any party who carries out processing or operates a communication to a third party in violation of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties. The court hearing the case may order the discontinuance of processing or notification that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court."

Article 8. Processing of legal data

(1) The processing of data for the purpose of criminal investigations and legal proceedings will be performed pursuant to the provisions of the *Code d'Instruction Criminelle*, the *Code de Procédure Civile*, the law relating to procedural regulations in administrative courts or other laws.

(2) The processing of data relating to offences, criminal convictions or security measures may be carried out only in performance of a legal provision.

(3) A complete compendium of criminal convictions can be held only under the auspices of the competent public authority.

(4) Any party acting privately who carries out processing in breach of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or only one of these penalties.

The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 9. Processing and freedom of expression

(Law of 27 July 2007)

(...) Without prejudice to provisions laid down in the Law of 8 June 2004 on the freedom of expression in the media and in as far as the undermentioned derogations are necessary to reconcile the right to privacy to the rules governing freedom of expression, processing carried out solely for journalistic, artistic or literary expression are not subject:

(a) - to the prohibition on processing the specific categories of data provided under Article 6, paragraph (1);

- to the limitations concerning the processing of legal data stated in Article 8,

(Law of 27 July 2007)

"if the processing is in connection with data that have manifestly been made public by the data subject, or to data which are directly related to the public life of the data subject or the event in which he is involved in a deliberate manner;"

(b) to the condition that the adequate protection required in the case of processing of data that is transferred to a third country as stated in Article 18 paragraph (1) should be provided;

(c) to the information obligation of Article 26, paragraph (1) if its application would compromise the collection of data from the data subject;

(d) to the information obligation of Article 26, paragraph (2) if its application would either compromise the collection of data, or a planned publication, or public disclosure in any form whatsoever of the said data, or would provide information that would make it possible to identify the sources of information;

(Law of 27 July 2007)

"(e) to the data subject's right of access which is deferred and limited in accordance with (...) Article 29, paragraph (3)."

(...)

Article 10. Processing for supervision purposes

(1) The data may only be processed for supervision purposes:

(a) if the data subject has given his consent, or

(b) in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary:

(Law of 27 July 2007)

"- for the safety of users and for the prevention of accidents, (...)

- for the protection of property, if there is a characteristic risk of theft or vandalism", or

(c) in private places where the resident natural or legal person is the controller, "or"

(Law of 27 July 2007)

"(d) if the processing is necessary to protect the vital interests of the data subject or of another where the data subject is physically or legally incapable of giving his consent."

(2) Data subjects will be informed by appropriate means such as signage, circulars and/or letters sent by registered post or electronic means of the processing stated in paragraph (1) letters (b) and (c). At the request of the data subject, the controller will provide the latter with the information stated in Article 26, paragraph (2).

(3) The data collected for supervision purposes may be communicated only:

(a) if the data subject has given his consent, except where forbidden by law, or

(b) to the public authorities as stated in Article 17, paragraph (1), or

(c) to the competent legal authorities to record a criminal offence or take legal action in respect of it and to the legal authorities before which a legal right is being exercised or defended.

(4) Any party that carries out processing in breach of the provisions of the paragraph (1) above will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of paragraph (1) of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 11. *abolished by the Law of 31 July 2006 and taken over by Article L.261-1 of the Employment Code*

(Law of 27 July 2007)

"Article 11 (new). Processing for the purposes of supervision at the workplace

(1) Processing for supervision reasons at the workplace may not be carried out by the employer if the employer is the controller except in the cases referred to in Article L.261-1 of the Employment Code."

Chapter III. Formalities prior to processing and advertising of processing

Article 12. Prior notification to the Commission Nationale

(1) (a) Apart from cases that fall within the scope of the provisions of Articles 8, 14 and 17, the controller will notify the Commission Nationale of the processing of data beforehand.

(b) Processing operations carried out by a single controller that are for identical or interlinked purposes may be contained in a single notification. In this case, the information required under Article 13 will be supplied for each processing operation only where it is specific to that operation.

(Law of 27 July 2007)

"(2) The following are exempt from the obligation to notify:

(a) processing, unless for the supervision purposes referred to in Article 10 above and Article L.261-1 of the Employment Code, carried out by the controller if that person appoints a data protection official. The data

protection official shall be responsible for establishing and forwarding to the Commission Nationale a register listing the processing operations carried out by the controller except those exempt from notification in accordance with paragraph (3) of the present Article and in accordance with the provisions relating to the disclosure of processing operations as provided under Article 15;

(b) processing operations for the sole purpose of keeping a register which, under a legal provision, is intended for public information purposes and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest;

(c) processing operations carried out by lawyers, notaries and process-servers and necessary to acknowledge, exercise or defend a right at law;

(d) processing carried out solely for journalistic, artistic or literary expression referred to in Article 9;

(e) processing necessary to protect the vital interests of the data subject or of another where the data subject is physically or legally incapable of giving his consent;

(3) The following are also exempt from the obligation to notify:

(a) The processing of data relating exclusively to personal data necessary for the administration of the salaries of persons in the service of or working for the controller, inasmuch as this data is used exclusively for the said administration of salaries and is only communicated to such persons as are entitled.

(b) The processing of data relating exclusively to the management of applications and recruitments and the administration of the staff in the service of or working for the controller.

The processing may not cover data on the health of the data subject, or sensitive or legal data within the meaning of Articles 6 and 8 of the Law, or data intended for assessing the data subject.

Such data may not be communicated to third parties except in the context of application of a provision of law or regulation, or if they are essential to achieving the objectives of the processing.

(c) The processing of data relating exclusively to the controller's bookkeeping, inasmuch as this data is used exclusively for such bookkeeping and the processing covers only the persons whose data is necessary for the bookkeeping.

Such data may not be communicated to third parties except in the context of application of a provision of regulation or law, or if such communication is essential to the bookkeeping.

(d) The processing of data referring exclusively to the administration of shareholders, debenture holders and partners, inasmuch as the processing covers solely the data necessary for such administration, the data covers only those persons whose data is necessary for such administration, and the data is not communicated to any third party except in the context of application of a provision of law or regulation.

(e) The processing of data relating exclusively to the management of the controller's client or supplier base.

The processing may only cover the controller's potential, current or former clients or suppliers.

The processing may not cover either data relating to the health of the data subject or sensitive or legal data within the meaning of Articles 6 and 8.

(f) The processing of data carried out by a foundation, an association or any other non-profit-seeking organisation in the context of their ordinary activities.

The processing must refer exclusively to the administration of its own members, persons with whom the controller maintains regular contact, or benefactors of the foundation, association or organisation.

This data may not be communicated to any third party except in the context of the application of a provision of law or regulation.

(g) The processing of identification data essential for communication carried out with the sole purpose of entering into contact with the party concerned, inasmuch as this data is not communicated to any third party.

Letter (g) shall only apply to the processing of data not covered by any of the other provisions of the present Law.

(h) The processing of data related exclusively to the recording of visitors carried out in the context of manual access control insofar as the data processed is restricted to only the name and business address of the visitor, his/her employer, his/her vehicle, the name, department and function of the person visited, and the time and date of the visit.

This data may only be used exclusively for manual access control.

(i) The processing of data carried out by educational establishments with a view to managing their relations with their pupils or students.

Processing covers exclusively data of a personal nature concerning potential, current or former pupils or students of the educational establishment.

This data may not be communicated to any third party except in the context of application of a provision of law or regulation.

(j) The processing of data of a personal nature carried out by administrative authorities if the processing is subject to specific regulations adopted by or by virtue of the law regulating access to the data processed and its use and the manner in which it is obtained.

(k) The processing of data of a personal nature necessary for the management of computerised and electronic communications systems and networks provided that it is not carried out for the purpose of supervision within the meaning of Article 10 and Article 11 (new).

(l) Processing carried out in accordance with Article 36 of the Law of 28 August 1998 on hospitals, except for the processing of genetic data.

(m) Processing carried out in accordance with Article 7, paragraph (1) of the present Law by a doctor concerning his/her patients, except for the processing of genetic data.

(n) Processing carried out by a pharmacist or a professional subject to the amended Law of 26 March 1992 on the exercise and enhancement of certain health professions. The processing of data of a personal nature relates exclusively to the supply of medicines and care or services provided. This data may not be communicated to a third party except in the context of the application of a provision of law or regulation."

(4) Any party that does not carry out the obligation to notify or supplies incomplete or inaccurate information is liable to a fine of between 251 and 125,000 euros. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 13. Content and form of the notification

(1) The notification will include at least the following information:

(Law of 27 July 2007)

(a) the name and address of the controller and of his representative (...), if any;

(b) the cause of legitimacy of the processing;

(c) the purpose or purposes of the processing;

(d) a description of the category or categories of data subjects and of the data or categories of data relating to them;

(e) the recipients or categories of recipients to whom the data might be disclosed;

(f) the third countries to which it is proposed to transfer the data;

(g) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Articles 22 and 23 to ensure security of processing.

(...) abolished by the Law of 27 July 2007

(2) Any amendment affecting the information stated in paragraph (1) must be notified to the Commission Nationale prior to the processing.

(Law of 27 July 2007)

"(3) Notification will be made to the Commission Nationale on paper accompanied, as appropriate, by a computerised document or an electronic transmission in a manner that it will establish. Acknowledgement of receipt of notification will be given.

A Luxembourg regulation sets forth the amount and methods of payment of the fee to be collected for any notification and amendment to a notification.

(4) Processing operations that have a single purpose relating to categories of identical data and intended for the same recipients or categories of recipients may be covered by a single notification to the Commission Nationale. In this case, the controller for each processing operation sends the Commission Nationale a formal undertaking of its compliance with the description that appears in the notification."

Article 14. Prior authorisation by the Commission Nationale

(Law of 27 July 2007)

"(1) Prior authorisation by the Commission Nationale will be required for:

(a) the processing of genetic data referred to in paragraph 3, letters (c) and (d) of Article 6;

(b) the processing operations for supervision purposes referred to in Article 10 if the data resulting from the supervision is recorded, and in Article 11 (new);

(c) the data processing operations for historical, statistical or scientific purposes referred to in Article 4, paragraph (2).

(d) the combination of data as referred to in Article 16;

(e) processing relating to the credit status and solvency of the data subjects if the processing is carried out by persons other than professionals of the financial sector or insurance companies in respect of their clients;

(f) processing involving biometric data necessary for checking personal identity;

(g) the usage of data for purposes other than those for which they were collected. Such processing may be carried out only where prior consent is given by the data subject or if it is necessary to protect the vital interest of the data subject."

(2) The request for authorisation will include at least the following information:

(Law of 27 July 2007)

(a) the name and address of the controller (...) "and where applicable" his representative (...);

(b) the cause of legitimacy of the processing;

(c) the purpose or purposes of the processing;

(d) the origin of the data;

(e) a detailed description of the data or the categories of data as well as of the proposed processing operations;

(f) a description of the category or categories of data subjects;

(g) the recipients or categories of recipients to whom the data might be disclosed;

(h) the third countries to which it is proposed to transfer the data;

(i) a detailed description to evaluate compliance with the security measures provided in Articles 22 and 23.

(...) abolished by the Law of 27 July 2007

"(3) Any amendment affecting the information referred to in paragraph (2) must be authorised by the Commission Nationale prior to carrying out the processing.

(4) The request for authorisation is made to the Commission Nationale on paper accompanied, as appropriate, by a computerised document or an electronic transmission. Acknowledgement of receipt of the request for authorisation will be given. A Luxembourg regulation shall set forth the amount and methods of payment of the fee to be collected for any authorisation and amendment to an authorisation."

(5) Processing operations that have a single purpose relating to categories of identical data and intended for the same recipients or categories of recipients may be authorised by a single decision of the Commission Nationale. In this case, the controller for each processing operation will send the Commission Nationale a formal undertaking of its compliance with the description that appears in the authorisation.

(6) Any party who carries out processing in breach of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 15. Disclosure of processing operations

(1) The Commission Nationale will hold a public register of processing operations.

(2) This register will include:

(a) processing operations notified to the Commission Nationale under Article 12, paragraph (1);

(b) processing operations authorised by the Commission Nationale under Article 14, paragraph (1); and

(Law of 27 July 2007)

"(c) processing operations supervised by the data protection official and forwarded to the Commission Nationale under Article 12, paragraph (2) letter (a) and this person's identity."

(3) The register held by the Commission Nationale will contain the information required respectively under Article 13, paragraph (1) and Article 14, paragraph (2) for each processing operation. For the processing operations subject to prior authorisation, the register also gives information on the authorisation issued by the Commission Nationale.

(4) Any person may examine free of charge the information contained in this public register which is available

on-line apart from that provided in Article 13, paragraph (1) letter (g) and Article 14, paragraph (2) letter (i).

(5) However, the Commission Nationale may restrict this disclosure if such a measure is necessary to safeguard:

(a) national security;

(b) defence;

(c) public safety;

(Law of 27 July 2007)

"(d) the prevention, tracking down and recording of criminal offences and the combating of money laundering;"

(e) a major economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters;

(f) the protection of the data subject or of the rights and freedoms of others;

(g) freedom of expression;

(h) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (c), (d) and (e); and

(i) professional secrecy and trade secrecy of the data subject and of the controller;

(6) The Commission Nationale will publish an annual report listing notifications and authorisations.

(7) This Article does not apply to processing operations the sole purpose of which is to keep a register which under a Luxembourg law or regulation is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

Article 16. Combination of data

(Law of 27 July 2007)

(1) The combination of data not expressly provided for by law "or regulation" must be authorised in advance by the Commission Nationale following a joint request presented by the relevant controllers.

(2) The combination of data must allow the achievement of legal or statutory objectives that are of legitimate interest for controllers, must not result in discrimination or the reduction of rights, freedoms and appropriate safeguards for the data subjects, must contain appropriate security measures and must take account of the type of data being combined.

(Law of 27 July 2007)

"(3) Combination is authorised only where the fact that the filing systems are for compatible purposes and the professional secrecy to which the controllers are bound, where applicable, are respected."

Article 17. Authorisation by regulatory means

(1) The following are subject to a Luxembourg regulation:

(a) processing operations of a general nature necessary for the prevention, tracking down and recording of criminal offences that are restricted to the Luxembourg police force, the *Inspection Générale de la Police* and the Customs and Excise authority in line with their respective legal and regulatory duties.

The Luxembourg regulation will determine the controller, the cause of legitimacy of the processing, the purpose or purposes of the processing, the category or categories of data subjects and the data or categories of data relating to them, the origin of these data, the third parties or categories of third parties to which these data may be disclosed and the measures to be taken to ensure secure processing pursuant to Article 22 of this Law.

(b) processing operations relating to State security, defence and public safety, and

(c) data processing operations in the area of criminal law carried out under international treaties or inter-governmental agreements or in the context of cooperation with the International Criminal Police Organisation (OIPC – Interpol).

(Law of 27 July 2007)

"(d) the creation and operation, for the purposes and under the conditions referred to under (a) above, of a video surveillance system for security areas, meaning any place to which the public has access that by its nature, location, configuration or frequentation presents a greater risk of criminal offences being committed.

Security areas shall be determined subject to the conditions provided for in a Luxembourg regulation."

(2) The monitoring and supervision of processing operations carried out pursuant wither to a provision of national law or an international treaty will be carried out by a supervisory authority made up of the *Procureur Général d'Etat* [State Prosecutor] or his deputy who will act as its chairman and two members of the Commission Nationale, appointed at the latter's proposal by the Minister.

The organisational structure and operations of the supervisory authority will be covered by a Luxembourg regulation.

The supervisory authority will be immediately informed of a data processing operation as referred to in this Article. It will ensure that the said processing operations are carried out in accordance with the legal provisions that govern them.

In order to perform its function, the supervisory authority will have direct access to the data processed. In respect of the processing operations carried out, it may perform on-site checks and obtain any information and documents required to perform its duties. It may also appoint one of its members to perform specific supervisory functions that will be carried out under the conditions stated above. The supervisory authority will make any necessary rectifications and deletions. Each year it will present a report on the performance of its function to the Minister.

The right of access to data referred to in this Article may be exercised only through the supervisory authority. The supervisory authority will carry out the appropriate verification and investigations, arrange for any necessary rectifications and will inform the data subject that the processing in question does not contain any data contrary to the treaties, laws and implementing regulations.

(3) Any party acting privately who carries out processing in breach of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Chapter IV. Transfer of data to third countries

Article 18. Principles

(1) Transfers to a third country of data that are the subject of processing, or that will be the subject of processing after their transfer, may take place only where the country in question provides an adequate level of protection and complies with the provisions of this Law and its implementing regulations.

(2) The adequacy of the level of protection afforded by a third country must be assessed by the controller in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particularly the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

(3) In the event of doubt, the controller will immediately inform the Commission Nationale which will consider whether the third country offers an adequate level of protection. In accordance with Article 20 the Commission Nationale will notify the European Commission of cases where it considers that the third country does not offer an adequate level of protection.

(4) If the European Commission or Commission Nationale finds that a third country does not have an adequate level of protection, transfer of data to that country will be prohibited.

(5) Any party who transfers data to a third country in violation of the provisions of paragraphs (1), (2) and (4) above will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of any transfer that is contrary to the provisions of paragraphs (1), (2) and (4) of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 19. Derogations

(1) The transfer of data or a set of data to a third country that does not offer an adequate level of protection within the meaning of Article 18, paragraph (2), may, however, take place, provided:

(a) the data subject has given his consent to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract to which the data subject and the controller are parties or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of a legal claim; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(Law of 27 July 2007)

(f) the transfer occurs from a public register as provided in "Article 12, paragraph (2) letter (b)."

(Law of 27 July 2007)

"(2) In the case of a transfer made to a third country that does not offer an adequate level of protection within the meaning of Article 18, paragraph (2), the controller must, at the request of the Commission Nationale, provide the Commission within fifteen days with a report stating the conditions under which it made the transfer."

(3) Without prejudice to the provisions of paragraph (1), the Commission Nationale may authorise, as a result of a duly reasoned request, a transfer or set of transfers of data to a third country that does not provide an adequate level of protection within the meaning of Article 18, paragraph (2) if the controller offers sufficient guarantees in respect of the protection of the privacy, freedoms and fundamental rights of the data subjects, as well as the exercise of the corresponding rights. These guarantees may result from appropriate contractual clauses. The controller is required to comply with the decision of the Commission Nationale.

(4) Any party who transfers data to a third country in violation of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties. The court hearing the case may order the discontinuance of a transfer that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 20. Reciprocal information

(Law of 27 July 2007)

"(1) The Commission Nationale will inform the Minister of any decision taken pursuant to Article 18, paragraphs (3) and (4), and Article 19, paragraph (3)."

(2) The Minister will inform the Commission Nationale of any decision relating to the level of protection of a third country taken by the European Commission.

Chapter V. Subordination and security of processing operations

Article 21. Subordination

Any person who acts under the authority of the controller or of the processor, including the processor himself, and who has access to data may not process them except on instructions from the controller, unless he is required to do so by law.

Article 22. Security of processing operations

(Law of 27 July 2007)

(1) The controller must implement all appropriate technical and organisational measures to ensure the protection of the data he processes against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. "A description of these measures and of any subsequent major change must be communicated to the Commission Nationale at its request, within fifteen days."

(2) If the processing is carried out on behalf of the controller, the latter must choose a processor that provides sufficient guarantees as regards the technical and organisational security measures pertaining to the processing to be carried out. It is up to the controller as well as the processor to ensure that the said measures are respected.

(3) Any processing carried out on another's behalf must be governed by a written contract or legal instrument binding the processor to the controller and providing in particular that:

(a) the processor will act only on instructions from the controller, and

(b) the obligations referred to in this Article will be also incumbent on the latter.

Article 23. Special security measures

Depending on the risk of the breach of privacy, as well as the state of the art and the costs associated with their implementation, the measures referred to in Article 22, paragraph (1) must:

(a) prevent any unauthorised person from accessing the facilities used for data processing (monitoring of entry to facilities)

(b) prevent data media from being read, copied, amended or moved by any authorised persons (monitoring of media);

(c) prevent the unauthorised introduction of any data into the information system, as well as any unauthorised knowledge, amendment or deletion of the recorded data (monitoring of memory);

(d) prevent data processing systems from being used by unauthorised person using data transmission facilities (monitoring of usage);

(e) guarantee that authorised persons when using an automated data processing system may access only data that are within their competence (monitoring of access);

(f) guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission);

(g) guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any person (monitoring of introduction);

(h) prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported (monitoring of transport);

(i) safeguard data by creating backup copies (monitoring of availability).

Article 24. Professional secrecy

(1) Members of the Commission Nationale and any other person who carries out duties at the Commission Nationale or on its behalf, as well the official in charge of data protection, are subject to the compliance with professional secrecy obligations as provided under Article 458 of the *Code Pénal* [Criminal Code] even after their duties have ceased.

(2) Officials in charge of data protection when carrying out these functions may not plead the professional secrecy to which they are subject to the Commission Nationale.

(3) Certified service providers may not plead the professional secrecy to which they are subject in accordance with Article 19 of the Law of 14 August 2000 relating to electronic commerce to the Commission Nationale.

(Law of 27 July 2007)

(4) Controllers acting within the framework of fulfilling their duties as specified in Article 7, "paragraphs (1) and (2)" may not plead the professional secrecy to which they are subject to the Commission Nationale if the latter has been instructed in accordance with Article 32, paragraphs (4) and (5).

Article 25. Sanctions relating to the subordination and security of processing operations

Any party who carries out a processing operation in breach of the confidentiality and security rules referred to in Articles 21, 22 and 23, will be liable to a prison sentence of between eight days and six months and a fine of between 251 and 125,000 euros or just one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of Article 21, 22 and 23, subject to a financial penalty the maximum amount of which will be set by the said court.

Chapter VI. Rights of the data subject

Article 26. The data subject's right to information

(1) When the data are collected directly from the data subject, the controller must supply the data subject, no later than the point at which the data are collected and regardless of the type of media used, with the following information unless the data subject has already been informed thereof:

(a) the identity of the controller and of his representative, if any;

(b) the purpose or purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients to whom the data might be disclosed;

- whether answering the questions is compulsory or voluntary, as well as the possible consequences of failure to answer;

- the existence of the right of access to data concerning him and the right to rectify them inasmuch as, in

view of the specific circumstances in which the data is collected, this additional information is necessary to ensure the fair processing of the data in respect of the data subject;

(...) abolished by the Law of 27 July 2007

(Law of 27 July 2007)

"inasmuch as, in view of the specific circumstances in which the data is collected, this additional information is necessary to ensure the fair processing of the data in respect of the data subject."

(2) Where the data have not been obtained from the data subject, the controller must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with the following information, except where the data subject already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purpose or purposes of the processing for which the data are intended;

(c) any further information such as

- the categories of data concerned;

- the recipients or categories of recipient of the data to whom the data might be disclosed;

- the existence of the right of access to data concerning him and the right to rectify them;

(...) abolished by the Law of 27 July 2007

(Law of 27 July 2007)

"inasmuch as, in view of the specific circumstances in which the data is collected, this additional information is necessary to ensure the fair processing of the data in respect of the data subject."

(3) Any party who is in breach of the provisions of this article will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 27. Exceptions to the data subject's right to information

(1) Article 26, paragraphs (1) and (2), do not apply when the processing is necessary to safeguard:

(a) national security;

(b) defence;

(c) public safety;

(Law of 27 July 2007)

"(d) the prevention, tracking down, recording and prosecution of criminal offences, including the combating of money laundering, or the progress of other legal proceedings;"

(e) an important economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters;

(f) protection of the data subject or the rights and freedoms of others;

(Law of 27 July 2007)

"(g) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in letters (c), (d) and (e).

(2) The provisions of Article 26 are subject to derogations if the data are collected in the cases provided for in Article 9, letters (c) and (d)."

(3) The provisions of Article 26 paragraphs (1) and (2) will not apply where, in particular for a processing operation for a statistical, historical or scientific purpose, it is not possible to notify the data subject or doing so entails disproportionate efforts, or if the recording or the notification of the data is provided by law.

(4) Any party in breach of the provisions of paragraphs (1) and (2) above will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of paragraphs (1) and (2) of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

Article 28. Right of access

(1) Upon application to the controller, the data subject or his beneficiaries who can prove they have a legitimate interest may obtain free of charge, at reasonable intervals and without excessive waiting periods:

(a) access to data on him;

(b) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;

(c) disclosure to him in an intelligible form of the data undergoing processing and of any available information as to their source;

(d) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 31;

(2) Any party who intentionally obstructs by any method whatsoever the exercise of the right of access will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties.

(3) Patients have the right of access to data on them. The right of access will be exercised by the patient himself or through a doctor he appoints. In the event of the patient's death, his non legally separated spouse and his children as well as any other person who at the time of the death has lived with him in his household, or in the case of minors, his father and mother, may exercise the right of access as stated in the previous paragraph through a doctor they have appointed.

The patient's right of access may still be exercised during the lifetime of a person under guardianship or trusteeship as set forth under the Law of 11 August 1982 though a doctor appointed by his guardian or trustee.

(...) abolished by the Law of 27 July 2007

(4) As appropriate, the controller will rectify, delete or block data the processing of which does not comply with this Law, in particular due to the incomplete or inaccurate nature of the data, subject to the penalty of a temporary or definitive ban on the processing or the destruction of these data under the conditions stated in Article 33.

(5) Any person who when exercising his right of access has realistic reasons for assuming that the data disclosed to him do not comply with the data processed may inform the Commission Nationale thereof and it will carry out the necessary checks.

(6) Any rectification, deletion or blocking carried out in accordance with paragraph (4) will be immediately notified by the controller to the recipients to whom the data have been disclosed unless this should prove impossible.

(7) Without prejudice to the sanction provided in paragraph (4), any party who intentionally breaches the provisions of this Article or any party who intentionally takes an assumed first name or surname or pretends to a false capacity to obtain disclosure of the data being processed pursuant to paragraph (1) will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties.

Article 29. Exceptions to the right of access

(1) The controller may restrict or defer exercise of a data subject's right of access if such a measure is necessary in order to safeguard:

(a) national security;

(b) defence;

(c) public safety;

(Law of 27 July 2007)

"(d) the prevention, tracking down, recording and prosecution of criminal offences, including the combating of money laundering, or the progress of other legal proceedings;"

(e) a major economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters;

(f) the protection of the data subject or the rights and freedoms of others;

(Law of 27 July 2007)

"(g) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official

authority in cases referred to in letters (c), (d) and (e);"

(...) abolished by the Law of 27 July 2007

(2) In the event that there is obviously no risk of breaching the privacy of a data subject, the controller may limit the right of access when the data are being processed solely for the purposes of scientific research, or are stored in data form for a period not exceeding that necessary for the sole purpose of establishing statistics, and the said data cannot be used for the purpose of taking a measure or a decision relating to specific persons.

(Law of 27 July 2007)

"(3) In the context of the processing of personal data carried out for journalistic, artistic or literary expression, everyone is entitled to access data concerning them. Nevertheless, in all cases, the data subject's right of access to the data concerning him used in the context of processing carried out for journalistic, artistic or literary expression is limited inasmuch as it may only cover information concerning the origin of the data making it possible to identify a source. Subject to this reservation, the data must be accessed through the intermediary of the Commission Nationale pour la Protection des Données in the presence of the Chairman of the Conseil de Presse or his representative, or the Chairman of the Conseil de Presse duly called upon."

(4) The controller must state the reason for which he is limiting or deferring exercise of the right of access.

When the right of access is deferred, the controller must state the date from which the right of access can again be exercised. The controller will notify the reason to the Commission Nationale.

(5) In the case of limitation of the data subject's right of access, the right of access will be exercised by the Commission Nationale which has investigative powers and arranges for the rectification, deletion or blocking of data the processing of which does not comply with this Law. The Commission Nationale may notify the data subject of the result of its investigations, while at the same time not endangering the purpose or purposes of the processing operations in question.

(6) Any party who is in breach of the provisions of paragraph (4) above will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties.

Article 30. The data subject's right to object

(1) Any data subject will be entitled:

(a) to object at any time, for compelling and legitimate reasons relating to his special situation, to the processing of any data on him except in cases where legal provisions expressly provide for that processing. Where there is a justified objection, the processing instigated by the controller may not involve those data;

(Law of 27 July 2007)

(b) to object upon request and free of charge to the processing "of data" on him proposed by the controller for the purpose of marketing; it will be incumbent on the controller to bring this right to the attention of data subject;

(c) to be informed before data on him are disclosed for the first time to third parties or used on behalf of third parties for marketing purposes and to be expressly offered the right to object to the said disclosure or usage free of charge.

(2) Any party who intentionally breaches the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of 251 to 125,000 euros or only one of these penalties.

Article 31. Individual automated decisions

A person may be subject to an individual automated decision producing legal effects on him if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view, or

(b) is authorised by law which also lays down measures to safeguard the data subject's legitimate interests.

Chapter VII. Monitoring and supervision of the implementation of the law

Article 32. Duties and powers of the Commission Nationale

(1) A supervisory authority named the "Commission Nationale pour la Protection des Données" has been set up in charge of monitoring and checking that data being processed are processed in accordance with the provisions of this Law and its implementing regulations.

2) Every year the Commission Nationale will submit a written report to the members of the Cabinet on the fulfilment of its duties. In this report it will cover in particular the status of notifications and authorisations, and the defects or misuses that are not specifically covered by the existing legal, regulatory and administrative provisions. It will publish its annual report. The report will be examined by the consultative commission on human rights, a consultative government body on human rights on Luxembourg territory whose membership and duties are set out in a Luxembourg regulation.

(3) The duties of the Commission Nationale are as follows:

(a) to ensure implementation of the provisions of this Law and its implementing regulations, in particular those relating to the confidentiality and security of processing operations;

(b) to receive notifications prior to the implementation of a processing operation and changes affecting the content of those notifications and to carry out ex post facto monitoring of the lawfulness of the processing operations notified; likewise it will be promptly informed of any processing subject to prior authorisation;

(c) to publicise the processing operations notified to it by keeping an appropriate register, unless otherwise provided;

(d) to authorise the implementation of processing operations subject to the system described in Article 14 of this Law;

(e) to be asked for its opinion on all draft or proposed laws relating to the creation of a processing operation as well as all regulatory or administrative measures issued on the basis of this Law. These opinions will be published in the annual report referred to in Article 15, paragraph (6);

(f) to present to the Government any suggestions that might simplify and improve the legislative and regulatory framework with regard to the processing of data;

(g) to receive and where applicable, following discussions with the authors, approve codes of conduct relating to a processing operation or a set of processing operations submitted to it by professional associations which represent the controllers;

(h) to advise the Government, either at the request of the latter or on its own initiative, regarding the consequences of developments in information processing technologies with regard to the respect of the freedoms and fundamental rights of individuals; to this end it may commission studies, surveys or expert reports;

(i) to promote, on a regular basis and by any method it deems fit, the dissemination of information relating to data subjects' rights and controllers' obligations, particularly as regards the transfer of data to third countries.

4) The Commission Nationale may be approached by any person, acting on his own behalf, through his lawyer or by any other duly authorised natural or legal person, with a request relating to respect of his fundamental rights and freedoms as regards a processing operation. The data subject will be informed of the outcome of the request.

(Law of 27 July 2007)

(5) The Commission Nationale may, in particular, be approached by any data subject with a request to check the lawfulness of a processing operation in the event of refusal or limitation of the exercise of the data subject's right of access in accordance with Article 29, "paragraph (5)" of this Law.

(6) If the Commission Nationale is approached by one of the persons or bodies referred to in Article L-261-1, paragraph (2) of the Employment Code, regarding a violation of that Article, it will give a ruling within a month of the referral.

(7) Under this Law, the Commission Nationale has the power to investigate under which it has access to data that are subject to the processing in question. It will collect all the information necessary for fulfilling its monitoring duties. To this end, it will have direct access to premises other than residential premises where processing takes places, as well as to the data that are being processed, and will carry out the necessary checks.

(8) The Commission Nationale is entitled to engage in legal proceedings in the interests of this Law and its implementing regulations. It will notify the legal authorities of any offences of which it is aware.

(9) The Commission Nationale will co-operate with its counterparts which are supervisory authorities set up in other Member States of the European Union to the extent required for them to perform their duties, notably by exchanging any appropriate information.

(10) The Commission Nationale will represent Luxembourg on the "group for the protection of individuals with regard to the processing of personal data" set up by Article 29 of Directive 95/46/EC;

(11) Any party who intentionally prevents or obstructs by any method whatsoever the performance of the duties incumbent upon the Commission Nationale will be liable to a prison sentence of between eight days and one year and fine of between 251 and 125,000 euros or just one of these penalties. Refusing its members access to premises other than residential premises where processing takes place, as well as to the data that

are being processed, or refusing to disclose any information and documents requested will be regarded as intentional prevention or obstruction of the performance of the duties incumbent on the Commission Nationale.

Article 33. Administrative sanctions

(1) The Commission Nationale may take the following disciplinary sanctions:

(a) alert or admonish controllers who have violated the obligations imposed upon them by Articles 21 to 24;

(b) block, delete or destroy data that have been subject to a processing operation contrary to the provisions of this Law or its implementing regulations;

(c) impose a temporary or definitive ban on a processing operation that is contrary to the provisions of this Law or to its implementing regulations;

(d) order publication of the prohibition decision in full or in extracts in newspapers or by any other method, at the cost of the person sanctioned.

(2) An appeal may be made against the above decisions pursuant to Article 3 of the Law of 7 November 1996 relating to the organisation of the administrative courts.

Article 34. Membership of the Commission Nationale

(1) The Commission Nationale is a public authority in the form of a Public Institution (*Etablissement Public*). Its headquarters are in Luxembourg City. The headquarters may be transferred at any time to any other location in Luxembourg pursuant to a Luxembourg regulation.

The Commission Nationale has a legal personality and has financial and administrative autonomy under the supervision of the Minister.

It carries out the duties with which it is invested under this Law in a totally independent manner.

(2) The Commission Nationale is made up of three permanent members and three substitute members appointed and dismissed by the Grand Duke at the proposal of the Cabinet. The President is appointed by the Grand Duke.

Members are appointed for a term of six years. This term may be renewed once.

On each occasion the Cabinet will suggest to the Grand Duke as a permanent and substitute member at least one legal specialist and one information technology specialist who have completed university studies.

Before taking up office, the President of the Commission Nationale will take the following oath before the Grand Duke or his representative: "I swear loyalty to the Grand Duke and obedience to the constitution and laws of the State. I promise to carry out my duties with integrity, precision and impartiality."

Before taking up office, members of the Commission Nationale will take the following oath before the Grand Duke or his representative: "I swear loyalty to the Grand Duke and obedience to the constitution and laws of the State. I promise to carry out my duties with integrity, precision and impartiality."

When the President or a permanent member of the Commission Nationale comes from the public sector, he will receive special leave for his term of office retaining all benefits and rights arising from his respective status. He will continue in particular to receive his pay, compensation or salary as appropriate, as well as enjoying the social security arrangements pertaining to his status.

(Law of 27 July 2007)

"For the purposes of the present article, pay, compensation or salary shall mean the emolument laid down for the various physical functions at the time of the appointment, including all increases for seniority, progress and promotions which the civil servant, employee or worker can claim under the provision of a law, under a provision of a regulation adopted by virtue of a law, and under the collective contract covering State workers if he had continued to be part of his original administration or establishment.

The term pay, compensation or salary does not include remittances, incidental entitlements, travel allowances, office or other costs if these are not considered, according to the provisions under which they are established, as constituting an integral part of the pay, compensation or salary.

(...)

In the event of termination of the term of office, the member concerned will at his request be reintegrated into his original department in a position corresponding to the grade and step reached at the end of his term of office."

If there is no vacancy, a new exceptional position with the same wage may be created; this position will automatically cease when a vacancy occurs for an appropriate ordinary position.

When the President or a permanent member of the Commission Nationale comes from the private sector, he

will receive remuneration calculated with reference to the regulations setting the relevant compensation of employees of State departments and services on the basis of an individual decision taken under Article 23 of the Luxembourg regulation of 28 July 2000 setting out the arrangements for the compensation of employees of State departments and services. He will continue to belong to the social security scheme which he was part of when carrying out his last occupation.

In the event of termination of the term of office, for a maximum period of one year he will receive transitional monthly compensation equal to the average monthly salary or pay in respect of the last contributory professional earnings pertaining to his current insurance history prior to the commencement of his duties as President or a permanent member of the Commission Nationale. That transitional compensation will be reduced where the party receives professional income or has a personal pension.

The President and permanent members of the Commission Nationale will receive special compensation reflecting the commitment required by their duties which will be set by Luxembourg regulation.

The resignation of a member of the Commission Nationale will automatically occur when he reaches the age limit of 65.

Substitute members will receive compensation the amount of which will be set by a Luxembourg regulation.

(3) Members of the Commission Nationale may not be members of the Government, the *Chambre des Députés*, the *Conseil d'Etat* or the European Parliament and may not carry out any professional activities, or directly or indirectly hold interests in a company or any other body involved in the field of data processing.

(4) If a member of the Commission Nationale ceases to carry out his duties during the course of his term of office, the term of office of his successor will be limited to the remaining outstanding period.

Article 35. Operation of the Commission Nationale

(1) The Commission Nationale will be a collegiate body. It will draw up its internal rules of procedure, including its working procedures and methods, within a month of being set up. The internal rules of procedure will be published in the *Mémorial*.

(2) Subject to the provisions of this Law, the internal rules of procedure will set forth:

(a) the rules of procedure applicable before the Commission Nationale,

(b) the rules of operation of the Commission Nationale,

(c) the organisation of the departments of the Commission Nationale.

(3) The permanent members of the Commission Nationale will be invited to attend meetings by the President. Meetings are properly called at the request of two permanent members. The invitation will contain the agenda.

Permanent members who are unable to attend a meeting are required to notify their substitutes and forward the invitation to them.

(4) The Commission Nationale may validly sit and deliberate only if there are three members present.

(5) Members of the Commission Nationale may not sit, deliberate or pass decisions on any matter in which they have a direct or indirect interest.

(6) Resolutions are passed by majority vote. Abstentions are not permitted.

(7) The Cabinet which has proposed the appointment of a member of the Commission Nationale may propose his dismissal to the Grand Duke. The opinion of the Commission Nationale will be heard before any dismissals.

(8) Whilst performing their duties, the members and substitute members of the Commission Nationale will not receive any guidance from any authority.

Art. 36. Status of members and employees of the Commission Nationale

(Law of 27 July 2007)

"(1) The executive staff of the Commission Nationale will include the following roles and positions:

a) in the higher career structure for *"attachés de direction"* (head office attaché), the seniority scale reference is: grade 12,
- *"conseillers de direction 1ère classe"* (senior head office consultant)
- *"conseillers de direction"* (head office consultant)
- *"conseillers de direction adjoints"* (assistant head office consultant)
- *"attachés de direction 1ers en rang"* (head office attaché, first rank)
- *"attachés de direction"* (head office attaché)

b) in the higher career structure for *"ingénieurs"* (engineers), the seniority scale reference is: grade 12,

- *"ingénieurs 1ère classe"* (senior engineers)
- *"ingénieurs chef de division"* (head of division engineers)
- *"ingénieurs principaux"* (chief engineers)
- *"ingénieurs-inspecteurs"* (engineer inspectors)
- *"ingénieurs"* (engineers)

c) in the normal career structure for *"ingénieurs techniciens"* (technical engineers), the seniority scale reference is: grade 7,

"ingénieurs techniciens inspecteurs principaux premiers en rang" (technical engineers, chief inspectors, first rank)
"ingénieurs techniciens inspecteurs principaux" (technical engineers, chief inspectors)
"ingénieurs techniciens inspecteurs" (technical engineers, inspectors)
"ingénieurs techniciens principaux" (chief technical engineers)
"ingénieurs techniciens" (technical engineers)

d) in the normal career structure for *"rédacteurs"* (junior executive officers), the seniority scale reference is: grade 7,

- "*inspecteurs principaux 1er en rang*" (chief inspectors, first grade)
- "*inspecteurs principaux*" (chief inspectors)
- "*inspecteurs*" (inspectors)
- "*chefs de bureau*" (head clerks)
- "*chefs de bureau adjoints*" (deputy head clerks)
- "*rédacteurs principaux*" (senior executive officers)
- "*rédacteurs*" (junior executive officers)

Officials in the career paths provided for above are State civil servants."

(2) The managerial staff provided in paragraph (1) above may be supplemented by both State white-collar employees and State blue-collar workers subject to the limits of the credit available.

The earnings of State employees are set in accordance with the Luxembourg ruling of 28 July 2000 setting out the arrangements for the compensation of employees of Government departments and services.

(3) The earnings and other compensation of all members, staff and employees of the Commission Nationale will be paid by the Commission Nationale.

(4) The Commission Nationale may in certain cases use external specialists whose services will be defined and paid for on the basis of an agreement under private law.

Article 37. Financial provisions

(1) Upon its formation, the Commission Nationale will receive initial funding of two hundred thousand euros from the State budget. The State will provide it with the movable and immovable property required to perform and carry out its duties properly.

(2) The financial year of the Commission Nationale will be the same as the calendar year.

(3) The Commission Nationale will draw up its operating account for the previous year and its annual report before 31 March each year. Before 30 September of each year, the Commission Nationale will draw up the budget for the next financial year. The budget, the annual accounts and reports drawn up will be sent to the Cabinet which will decide whether to discharge the Commission Nationale in respect of its duties. The decision confirming that the Commission Nationale has been discharged of its duties and the annual accounts of the Commission Nationale will be published in the *Mémorial.*

(Law of 27 July 2007)

(4) The Commission Nationale is authorised to deduct the equivalent of the costs of its serving staff and its operational expenses from the fees collected as provided "in Articles 13 and 14". In respect of the balance of the expenses still to be covered pursuant to its duties under this Law, the Commission Nationale will receive funding at an amount to be set on an annual basis and included in the State budget.

(5) abolished by the Law of 27 July 2007

Chapter VIII. Judicial remedies

Article 38. General provisions

Without prejudice to the criminal sanctions introduced by this Law and the actions for damages governed by ordinary law, in the event of a processing operation that violates formalities provided for under this Law being undertaken, any person is entitled to legal remedies as stated hereafter.

Art. 39. Action for discontinuance

(1) At the petition of

- the State Prosecutor who has instigated public action for the violation of this Law,

- by the Commission Nationale, should a disciplinary sanction as referred to in Article 33 of this Law, against which has been no appeal or which has been upheld by the administrative court, not have been complied with,

or

- by an injured party, should the Commission Nationale not have declared itself in respect of a claim made on the basis of Article 32, paragraph (4), (5) or (6) of this Law, the presiding judge of the district where the processing operation was carried out, or the judge who replaces him, will order the discontinuance of processing that is contrary to the provisions of this Law and the temporary suspension of the activity of the controller or processor. The presiding judge of the district where the processing operation is being carried out, or the judge who replaces him, may order the temporary closure of the business of the controller or processor if its sole activity is to process data.

(2) The action will be admissible even when the illegal processing has ceased or is not likely to recur.

(3) The action will be introduced and heard in summary proceedings in accordance with Articles 932 to 940 of the *Nouveau code de procédure civile*. However, by way of derogation to Article 939, paragraph 2, of the *Nouveau code de procédure civile*, no application may be made to set the summary proceedings aside.

(4) Articles 2059 and 2066 of the Code Civil will also apply.

(5) Publication of the decision in full or in extracts may be ordered in newspapers or by any other method, at the cost of the offender. Publication may be made only by virtue of a legal decision passed *res judicata*.

(6) Temporary suspension and, where applicable, temporary closure may be ordered independently of the public action. Temporary suspension or temporary closure ordered by the presiding judge of the district court or by the judge who replaces him will, however, cease in the event of a discharge or acquittal, and no later than the expiry of a period of two years from the date of the initial suspension or closure decision.

Chapter IX. The data protection official

Article 40. The data protection official

(Law of 27 July 2007)

(1) Any controller may (...) appoint a data protection official whose identity he will notify to the Commission Nationale.

(2) The powers of the data protection official are as follows:

(a) investigative powers to ensure supervision of the controller's compliance with the provisions of this Law and its implementing regulations;

(b) a right to be informed by the controller and a correlative right to inform the controller of the formalities to be carried out in order to comply with the provisions of this Law and its implementing regulations.

(Law of 27 July 2007)

"(3) In the performance of his duties, the data protection official is independent of the controller who appoints him.

In order to carry out his tasks the data protection official must be allowed adequate time.

There must be no possibility of the missions of activities being carried out concurrently by the data protection official being likely to cause a conflict of interest with the exercise of his mission.

(4) The data protection official may not be the subject of reprisals on the part of the employer as a result of the exercise of his missions, except in the case of a breach of his legal or contractual obligations."

(5) The data protection official will consult the Commission Nationale in the event of doubt regarding the compliance with this Law of a processing operation under his supervision.

(6) Natural or legal persons who are approved by the Commission Nationale may be appointed to the post of data protection official.

(Law of 27 July 2007)

(7) Approval for the activity of data protection official will be subject to proof of completion of university studies in law, economics, commercial management, natural science or information technology (...).

(8) By way of derogation to the previous paragraph, members registered in the following controlled

professions can be approved unconditionally as data protection officials: barristers, auditors (*réviseurs d'entreprises*), accountants (*experts-comptables*), doctors.

A Luxembourg regulation may add to this list other controlled professions that are subject to a supervisory or disciplinary body, either an official body or one specific to the profession and recognised by law.

(9) The Commission Nationale will check the qualities of all data protection officials. It may at any time object to the appointment or continuance of the data protection official if he:

(a) does not have the qualities required for the position of data protection official, or

(b) is already in contact with the controller in connection with activities other than the processing of data and this contact gives rise to a conflict of interests limiting his independence.

In the event of objection by the Commission Nationale, the controller will have three days to appoint a new data protection official.

(10) The Commission Nationale will define the methods of continuous monitoring of the qualities required for the position of data protection official.

(11) A Luxembourg regulation will set forth the methods for the appointment and dismissal of the data protection official, the performance of his duties and his relations with the Commission Nationale.

Chapter X. Specific, transitional and final provisions

Article 41. Specific provisions

(1) (a) The competent authorities referred to in Articles 88-1 to 88-4 of the *Code d'instruction criminelle* [Criminal Code], and

(b) the authorities acting in connection with a flagrant offence or in connection with Article 40 of the *Code d'Instruction Criminelle* will have automatic access on request and through the *Institut Luxembourgeois de Régulation* (hereinafter "ILR") to the data on the identity of subscribers and users of both electronic communications operators and suppliers and the postal services and the suppliers of these services.

(Law of 27 July 2007)

"The "112" emergency services centre, the emergency call centres of the Grand Duchy's police force, and the fire and rescue services of the City of Luxembourg will have access under the same terms and conditions as the authorities stated in the previous paragraph solely to the data on the identity of subscribers and users of electronic communications operators and suppliers."

(2) To this end, operators and suppliers will automatically provide the ILR free of charge with the data described in paragraph (1). The data must be updated at least once a day. Access must be guaranteed twenty-four hours per day seven days a week. A Luxembourg regulation will determine the electronic communications and postal services for which the service operators and suppliers need to make data available as well as the nature, format and methods of making the data available.

(Law of 27 July 2007)

"(3) Automatic access is restricted to special supervision measures as provided for in Articles 88-1 to 88-4 of the *Code d'instruction criminelle*, those taken in respect of flagrant offences or pursuant to Article 40 of the *Code d'Instruction criminelle* and the specific emergency measures provided in connection with the activities of the "112" emergency services centre, the emergency call centres of the Grand Duchy's police force, and the fire and rescue service of the City of Luxembourg."

(4) The procedure will be fully automated pursuant to authorisation by the Commission Nationale. The Commission Nationale will check in particular that the information system used is secure. That automation will allow remote access by electronic communication.

(Law of 27 July 2007)

"(5) The supervisory authority referred to in Article 17, paragraph (2) of the present Law shall ensure observance of the present Article."

Article 42. Transitional provisions

(1) Processing operations in automated or non-automated filing systems existing prior to introduction of this Law must be made to conform with the provisions of Chapter II and Chapter VI within a period of two years with effect from the introduction of this Law.

(2) However, any data subject may obtain on request, particularly with respect to the exercise of his right of

access, the rectification, deletion or blocking of data that are incomplete, inaccurate, or kept in a manner that is incompatible with the legitimate purposes pursued by the controller.

(3) The Commission Nationale may allow data kept solely for historical research purposes to be dispensed from compliance with paragraph (1).

(Law of 27 July 2007)

"(4) For application of the provisions of Article 34 above, the remuneration of the official appointed on 14 October 2002 as an effective member of the Commission Nationale pour la Protection des Données who holds a university qualification in information technology is determined by supposing that a fictitious appointment to the position of an *"attaché de gouvernement"* was made on 1 November 2002, that he had the benefit of promotion to the function of *attaché de gouvernement premier en rang"* on 1 November 2005, and that he would have the benefit of promotion to the function of *"conseiller de direction adjoint"* on 1 November 2008 at the earliest."

Article 43. Effectiveness of the transitional provisions

(1) The Commission Nationale will establish a notification schedule as provided in Article 13 paragraph (3) within four months of the date when its members are appointed. It will inform the public by means of publication in the *Mémorial* and a press release to newspapers published in Luxembourg of the date from which the notification schedule will be available at the Commission Nationale.

(2) Controllers will proceed to notify their processing operations within four months of the date of the official publication mentioned in paragraph (1).

(3) Controllers whose processing operations are authorised under a Luxembourg regulation or ministerial decree "authorising the creation and operation of a data bank" when this Law comes into force will notify or request authorisation of their processing operations only on the expiry of the period of validity of the authorisation granted, unless they consider it necessary to do so beforehand for reasons of compliance with the provisions of this Law.

(4) Non-automated processing operations involving data contained in or likely to appear in a filing system must be notified within twelve months of the date of the official publication mentioned in paragraph (1).

Article 44. Final provisions

(1) The amended law of 31 March 1979 governing the usage of name data in computer processing is repealed.

(2) In so far as they are not contrary to the provisions of this Law, regulations made in performance of the aforementioned amended Law of 31 March 1979 will remain in force until they are replaced by new provisions.

(Law of 27 July 2007)

"(3) Article 4, paragraph (3), letter d) of the Law of 30 May 2005 on the protection of privacy in the electronic communications sector must be amended as follows:

- in the first paragraph, the sentence ending "in order to furnish proof of a commercial transaction" should read "in order to furnish proof of a commercial transaction or of any other commercial communication";

- in the second paragraph, the first sentence should start thus: "The parties to the transactions or to any other commercial communications ...".

(4) In Article 5, paragraph (1), letter a), and Article 9, paragraph (1), letter a) of the Law of 30 May 2005 on the protection of privacy in the electronic communications sector, the duration of "12 months" is replaced by that of "6 months".

(5) The following additions shall be made at the end of Article 12 of the Law of 30 May 2005 concerning the protection of privacy in the electronic communications sector: "(...) without prejudice to application of Article 8 of the amended Law of 2 August 2002 on the protection of persons in respect of the processing of personal data".

(6) Article 23 of the Law of 8 June 2004 on freedom of expression in the media is amended to read as follows:

In point 1 of paragraph (2), the ending "including in the field of the processing of personal data" is added after the words "and editors".

In point 2 of the same paragraph, the following words "including complaints concerning respect for the rights and freedoms of persons regarding the processing of personal data" are added between the words "through any of the media" and "without prejudice to reserved powers"."

Article 45. Effectiveness

This law will be effective on the first day of the fourth month following its publication in the *Mémorial*. By way of derogation to the above, Articles 34, 35, 36 and 37 will be effective three days after the publication of this Law in the *Mémorial*.

Data Protection Technical Guidance
Determining what is personal data

Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

This technical guidance note explains and illustrates the Information Commissioner's view of what is personal data for the purposes of the Data Protection Act 1998. It is designed to help data protection practitioners decide whether data falls within the definition of personal data in circumstances where this is not obvious.

Preface

We have been aware for some time of the need to replace our guidance on the implications of the Durant judgment. Inevitably that guidance reflected the fact that the Court of Appeal was widely understood to have adopted a rather narrower interpretation of "personal data" and "relevant filing system" than most practitioners and experts had followed previously. We recognised the need to produce guidance with a greater emphasis on what is covered than what is not. In June 2007 the Article 29 Working Party, an advisory committee composed of representatives of the national supervisory authorities, agreed an opinion on the "concept of personal data". Though our guidance is structured differently we are satisfied that it is consistent with the approach taken by the Working Party. Both the Opinion and our guidance make great use of practical examples to illustrate the key considerations when deciding what is personal data.

Our previous guidance covered the meaning of both "personal data" and "relevant filing system". This guidance covers only "personal data". We intend in the near future to publish guidance on the meaning of "relevant filing system". In the mean time we are retaining the appendix to our previous guidance, Frequently Asked Questions on "relevant filing systems". This includes the "temp test" to help organisations decide whether they hold information within a "relevant filing system".

v1.0
21.08.07

Contents

Appendix

Data Protection Technical Guidance
Determining what is personal data

Introduction

The Data Protection Act 1998 (the DPA) applies only to information which falls within the definition of 'personal data'. The ICO, with other European data protection authorities, has been considering what is meant by 'personal data' in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the European Data Protection Directive or the Directive). This work has culminated in Opinion 4/2007 on the concept of personal data (01248/07/EN – WP136) adopted by the Article 29 Data Protection Working Party on 20 June 2007. This guidance draws on Opinion 4/2007 and applies the concepts discussed in that paper in a UK context.

Personal data as defined by the Directive and the Data Protection Act 1998

The Directive

The object of the European Data Protection Directive[1], implemented in the UK by the DPA, is to provide that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

'Personal data' is defined in Article 2 of the Directive by reference to whether information relates to an identified or identifiable individual.

The Directive provides, in Article 3, that it applies only to the processing of personal data where the processing is wholly or partly by automatic means, or where it is non-automated processing of personal data which forms part of a 'filing system[2]' or is intended to form part of a 'filing system'.

The Directive therefore considers first whether the information relates to an identifiable individual and then describes the two different types of processing (processing by automatic means or non-automated processing within a 'filing system') which will bring information within the scope of the Directive.

The Data Protection Act 1998

The DPA repeats the substance of the Directive definition of 'personal data' but tackles the definition in reverse order to the Directive. The DPA first considers the nature of the processing to determine whether the information in question is 'data' (either processed by automatic means or non-automated

[1] See Article 1 European Directive
[2] As defined in European Directive Article 2 (c)

processing within a filing system) and, secondly, considers whether the 'data' is 'personal data' in that it relates to an identifiable individual.

The Directive and the DPA cover two common categories of information:

- information processed, or intended to be processed, wholly or partly by automatic means (that is, information in electronic form)[3]; and

- information processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system)[4].

In most circumstances it will be relatively straightforward to determine:

(a) whether the processing falls within the scope of the Directive and the definition of 'data' in the DPA; and

(b) whether the information in question 'relates to' an 'identifiable individual';

and consequently, to determine whether you are processing 'personal data'.

In most cases it will be obvious when you are processing personal data. In those relatively few cases where this is unclear, this guidance, and in particular the questions set out in the flowchart, aim to take you through the factors to consider when determining whether you are processing personal data. The guidance offers suggestions, for use in appropriate cases, of considerations which may help you reach a decision about the nature of the information in question.

The additional scope of the Data Protection Act

The DPA introduces two more types of manual processing of information which, if the information relates to an identifiable individual, will involve processing of 'personal data'. These additional categories of processing are introduced in the DPA definition of 'data' and concern:

- processing information as part of an 'accessible record'[5]; and

- processing recorded information held by a public authority (referred to as 'category 'e' data' as it falls within paragraph (e) of the DPA section 1(1) definition of 'data').

The DPA is therefore concerned with four types of data which can be broadly referred to as:

[3] Data in electronic form is defined in section 1(1)(a) of the DPA.
[4] 'Relevant filing system' is defined in section 1(1)(a) DPA.
[5] 'Accessible record' is defined in section 1(1)(d) and section 68 DPA.

(i) electronic data;

(ii) data forming part of a relevant filing system;

(iii) data forming part of an accessible record (other than those accessible records falling within (i) or (ii) above); and

(iv) data recorded by a public authority.

The aim of this guidance and flowchart

Whether information falls within any of the four categories of 'data' covered by the DPA is considered in our guidance 'What information is 'data' for the purposes of the DPA?'

This guidance aims to help you determine whether 'data' is 'personal data' for the purposes of the DPA and the Directive. The guidance is in the form of a flowchart of numbered questions which, when taken in order, aim to assist in identifying 'personal data'. The flowchart questions are supplemented by guidance and illustrative examples aimed at developing a practical understanding of the concept of personal data.

Is the 'data' 'personal data' for the purposes of the Data Protection Act?

There are several steps to determining whether data (electronic or manual) is 'personal data'[6] for the purposes of the DPA. Questions to help you are set out in boxes 1 to 8 below[7].

1 Identifiability

Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the data controller?

Yes	Go to next question.
No	The data is not personal data for the purposes of the DPA.

See definition of 'personal data' section 1(1) DPA.
See also p. 6-8 Legal Guidance.

An individual is 'identified' if you have distinguished that individual from other members of a group. In most cases an individual's name together with some other information will be sufficient to identify them.

---

6 See definition of 'personal data' section 1(1) DPA.

7 See also p. 5-7 Legal Guidance

A name is the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context. By itself the name John Smith may not always be personal data because there are many individuals with that name. However, where the name is combined with other information (such as an address, a place of work, or a telephone number) this will usually be sufficient to clearly identify one individual[8]. (Obviously, if two John Smiths, father and son, work at the same place then the name, John Smith, and company name alone will not uniquely identify one individual, more information will be required).

Simply because you do not know the name of an individual does not mean you cannot identify that individual. Many of us do not know the names of all our neighbours, but we are still able to identify them.

Example: The tall, elderly man with a dachshund who lives at number 15 and drives a Porsche Cayenne.

Example: A description of an individual may be personal data where it is processed in connection with a neighbourhood watch scheme or by the police, when seeking to identify potential witnesses to an incident.

There will be circumstances where the data you hold enables you to identify an individual whose name you do not know and you may never intend to discover.

Example: Where an individual is not previously known to the operators of a sophisticated multi-camera town centre CCTV system, but the operators are able to distinguish that individual on the basis of physical characteristics, that individual is identified. Therefore, where the operators are tracking a particular individual that they have singled out in some way (perhaps using such physical characteristics) they will be processing 'personal data'.

Similarly, a combination of data about gender, age, and grade or salary may well enable you to identify a particular employee even without a name or job title.

Sometimes it is not immediately obvious whether an individual can be identified or not, for example, when someone holds information where the names and other identifiers have been removed. In these cases, Recital 26 of the Directive states that, whether or not the individual is nevertheless identifiable will depend on "all the means likely reasonably to be used either by the controller or by any other person to identify the said person".

---

[8] The term 'personal data' undoubtedly covers the name of a person in conjunction with his telephone number or information about his working conditions or hobbies – Paragraph 24 of the Opinion of Advocate General Tizzano in the Lindqvist case (Bodil Lindqvist v Aklagarkammaren i Jonkoping – Case Commissioner-101/01 – European Court of Justice) dlivered on 19 September 2002

Therefore, the fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the data subject is identified is not sufficient to make the individual identifiable for the purposes of the Directive. The person processing the data must consider all the factors at stake.

The starting point might be to look at what means are available to identify an individual and the extent to which such means are readily available. For example, if searching a public register or reverse directory would enable the individual to be identified from an address or telephone number, and this resource is likely to be used for this purpose, the address or telephone number data should be considered to be capable of identifying an individual.

When considering identifiability it should be assumed that you are not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals. Examples would include investigative journalists, estranged partners, stalkers, or industrial spies.

Means of identifying individuals that are feasible and cost-effective, and are therefore likely to be used, will change over time. If you decide that the data you hold does not allow the identification of individuals, you should review that decision regularly in light of new technology or security developments or changes to the public availability of certain records.

Taking this into account, a person who puts in place appropriate technical, organisational and legal measures to prevent individuals being identifiable from the data held may prevent such data falling within the scope of the Directive.

2 Meaning of 'relates to'

Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?	
Yes	The data is 'personal data' for the purposes of the DPA.
No	The data is not 'personal data' for the purposes of the DPA.
Unsure	See 3 to 8 below.
See definition of 'personal data" in section 1(1) DPA.	

It will often be clear where data 'relates to' a particular individual. However, sometimes this is not so clear and it may be helpful to consider in more detail what is meant by 'relates to'. Data which identifies an individual, even without a name associated with it, may be personal data where it is processed to learn or record something about that individual, or where the processing of

that information has an impact upon that individual. Therefore, data may 'relate to' an individual in several different ways, the most common of which are considered below.

3.1 Data 'obviously about' a particular individual

Is the data 'obviously about' a particular individual?	
Yes	The data is 'personal data' for the purposes of the DPA.
No	Go to next question.

Example: A medical history, a criminal record, or a record of a particular individual's performance at work or in a sporting activity.

With these types of information it is the content of the information that determines that it 'relates to' an individual.

3.2 Data that is not 'obviously about' a particular individual

There are many examples of records which will clearly be personal data where the information in question is not 'obviously about' an individual but is about their activities.

Example: Data such as personal bank statements or itemised telephone bills will be personal data about the individual operating the account or contracting for telephone services.

Where data is not 'obviously about' an identifiable individual the following question may help to determine whether the data is 'personal data'.

Is the data being processed, or could it easily be processed, to:

- **learn;**
- **record; or**
- **decide**

something about an identifiable individual,

or;

as an incidental consequence of the processing, either:

- **could you learn or record something about an identifiable individual; or**

- **could the processing have an impact on, or affect, an identifiable individual?**

Questions 4 to 8 may help when considering this issue.

4 Data linked to an individual

Is the data 'linked to' an individual so that it provides particular information about that individual?	
Yes	The data is 'personal data' for the purposes of the DPA.
No	Go to next question.

There will also be many cases where data is not in itself personal data but, in certain circumstances, it will become personal data where it can be linked to an individual to provide particular information about that individual.

Example: Data about the salary for a particular job may not, by itself, be personal data. This data may be included in the advertisement for the job and will not, in those circumstances, be personal data. However, where the same salary details are linked to a name (for example, when the vacancy has been filled and there is a single named individual in post), the salary information about the job will be personal data 'relating to' the employee in post.

5 The purpose of the processing

Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?	
Yes	The data is 'personal data' for the purposes of the DPA.
No	Go to next question.

5.1 Informing or influencing decisions

There are many other examples of data which 'relate to' a particular individual because it is linked to that individual and informs or influences actions or decisions which affect an individual.

Example: Data about an individual's phone or electricity account clearly determines what the individual will be charged.

Context is important here. Information about a house is often linked to an owner or resident and consequently the data about the house will be personal

data about that individual. However, data about a house will not, by itself, be personal data.

Example: Information about the market value of a particular house may be used for statistical purposes to identify trends in the house values in a geographical area. The house is not selected because the data collector wishes to know anything about the occupants, but because it is a four bedroom detached house in a medium-sized town. As soon as data about a house is either:

- linked to a particular individual, for example, to provide particular information about that individual (for example, his address) (see 4 above); or

- used in deliberations and decisions concerning an individual (even without a link to the individual's name, for example, the amount of electricity used at the house is used to determine the bill the individual householder is required to pay);

then that data will be personal data.

In both these examples the data about the house relates to the individual because the purpose of processing that data is to learn something about the individual (his address) or to determine something about him (the extent of his liability).

Example: Data used in deliberations or decisions about an individual may include data about unauthorised alterations to a house in breach of planning law where that data is processed to determine whether to prosecute the individual house owner. The data about the unauthorised alterations may be processed by reference to the house address but the data clearly relates to the individual who carried out the alterations in that the data is being processed to determine whether to take action against that person.

Example: Where the value of a particular house is used to determine an individual liability for Council Tax, or is used to determine the assets of an individual or individuals in proceedings following divorce, then this will be personal data because the data about the house is clearly linked to the individual or individuals concerned.

Example: A utility company may not record the name of the occupier of the house to which it provides water, but may simply note the address of the property and address all bills to 'the occupier'. Data concerning the water consumption for a particular address will be personal data about the occupier in that this data determines what that individual will be charged.

In this last example, even without a name associated with the water consumption data, this data will be personal data in that it determines what the occupier will be charged and the occupier is identified, even without a name, as the person living at the property in question and is therefore distinguished from other individuals. Also, if necessary, the water company is likely to be able to easily obtain the name of, if not the occupier, then at least the registered owner of the property.

5.2 Different organisations processing the same data for different purposes

It is important to remember that the same piece of data may be personal data in one party's hands while it may not be personal data in another party's hands.

Example: At New Year celebrations in Trafalgar Square two almost identical photographs of the revellers are taken by two separate photographers and stored in electronic form on computer. The first photographer, a photo journalist, takes a picture of the crowd scene to add to his photo library. The second photographer is a police officer taking photos of the crowd scene to identify potential troublemakers. The data in the electronic image taken by the journalist is unlikely to contain personal data about individuals in the crowd as it is not being processed to learn anything about an identifiable individual. However, the photo taken by the police officer may well contain personal data about individuals as the photo is taken for the purpose of recording the actions of individuals who the police would seek to identify, if there is any trouble, so they can take action against them.

A single piece of data, which is not personal data for one data controller may become personal data when it is passed to another data controller.

Example: An estate agent takes a photograph of a high street shop to market the property. The photograph is held in digital form by reference to its address or by reference to the client name on the agent's computer. The photograph is used solely to produce photographic prints to display and distribute to potential purchasers.

The photograph of the shop includes images of pedestrians who were walking past the shop at the time the photo was taken. The estate agent is not processing the shop data to learn anything about any of the pedestrians whose images were captured by chance on the photo, nor is it likely that the estate agent would ever process the photo for that purpose. The estate agent is unlikely to possess the appropriate software to digitally enhance the photo to identify individuals. Therefore, in the hands of the estate agent, the photo does not contain personal data about the pedestrians as it is not

processed to learn something about those individuals and nor is it likely to be processed by the estate agent for this purpose.

If we consider the example of the data contained in the images of the pedestrians captured on the shop photo by the estate agent in the above example, in certain circumstances, this data may be personal data about the pedestrians in the hands of another data controller.

Example: If, at about the same time as the photograph was taken by the estate agent, a bank raid took place on the same high street, the police might make a public appeal for information about movement on the high street at that time. The estate agent might supply the police with a copy of the photo in response to the appeal. The police would then process the digital photo, not to learn anything about the shop but, using photo enhancing technologies, to attempt to identify potential witnesses or suspects. The photo would then be being processed to learn something about the individual pedestrians and, in the hands of the police, may be personal data about such individuals

Therefore, data may not be personal data in the hands of one data controller (for example, the estate agent) but the same data may be personal data in the hands of another data controller (for example, the police) depending on the purpose of the processing and the potential impact of the processing on individuals.

6 Biographical significance

Does the data have any biographical significance in relation to the individual?	
Yes	The data is likely to be personal data for the purposes of the DPA.
No	Go to next question.
Unsure	Go to next question.

It is important to remember that it is not always necessary to consider 'biographical significance' to determine whether data is personal data. In many cases data may be personal data simply because its content is such that it is 'obviously about' an individual. Alternatively, data may be personal data because it is clearly 'linked to' an individual because it is about his activities and is processed with the purpose of determining or influencing the way in which that person is treated. You need to consider 'biographical significance' only where information is not 'obviously about' an individual or clearly 'linked to' him.

When considering 'biographical significance', what is important is whether the data go beyond recording the individual's casual connection with a matter or event which has no personal connotations for him. Does the processing of this data affect, or is it likely to affect, the individual? Data may, for example, have personal connotations for an individual if it provides information about an individual's whereabouts or actions at a particular time.

Example: Where an individual is listed as an attendee in the minutes of a meeting then the minutes will have biographical significance for the individual in that they record the individual's whereabouts at a particular time.

The fact that an individual attended the meeting will be personal data about that person. However, this does not mean that everything in the minutes of that meeting is personal data about each of the attendees.

Whether the content of the minutes includes any additional personal data, beyond attendance data, about the attendees at the meeting may be determined by the focus of the minutes.

7 Does the information concentrate on the individual?

Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?	
Yes	The data are likely to be personal data for the purposes of the DPA.
No	Go to next question.
Unsure	Go to next question.

Again, it is important to remember that it is not always necessary to consider 'focus' to determine whether data is personal data. In many cases data may be personal data because it is 'obviously about' an individual, or because it is clearly 'linked to' an individual because it is about the individual's activities.

You need to consider the 'focus' of the data only where information is not 'obviously about' an individual or clearly 'linked to' them.

7.1 Minutes of Meetings

It is often difficult to determine whether the contents of minutes of a meeting are personal data about either those attending the meeting or individuals whose conduct or condition is discussed at the meeting. Considering the

'focus' of the minutes may help determine whether any personal data is involved.

There will be circumstances where part of the record of a meeting will be personal data as the data is 'obviously about' or clearly 'linked to' an individual.

Example: Where an individual's suitability for a particular course or post is discussed (consideration being given to the individual's qualifications, personality and/or performance at work), the record of these discussions will be personal data about the individual in question.

In this last example, where a candidate's suitability for the job is only one of many topics discussed at the meeting, the whole of the record of the meeting will not necessarily be personal data about that candidate.

Example: Where a meeting is held to consider four candidates for a job, only the information which concentrates on the individual in question will be personal data about that individual. Information about other candidates, the need for a new person in the job or the creation of the new job, (that is, information which does not concentrate on the individual in question) will not be personal data about that individual. The minutes may therefore contain four separate sets of personal data about the four candidates respectively as well as information which is not personal data as it concerns the business requirement for the new employee.

If the whole of a meeting is about a particular individual then, assuming the minutes are held as data, they will be personal data about that individual. The meeting may concern the behaviour and actions or the condition of an individual. The personal data will include not only those facts about the condition or behaviour of the individual discussed at the meeting, but also any third parties' opinions about the individual in question and any indication of the intentions of any person in respect of that individual. These expressions of opinion or intention are personal data of the individual being discussed[9].

Example: A disciplinary hearing is held into the conduct of an individual employee. Everything discussed at the meeting is likely to be personal data about the individual in question. This will include the statements of fact about the employee's behaviour; opinions about the employee; and statements as to any proposed disciplinary measures provided by colleagues. The minutes of this meeting will be personal data about the individual as the information is clearly linked to the behaviour, condition or activities of the individual in question.

[9] DPA section 1(1) – 'personal data'

Where comments made at a meeting are, in the minutes, directly attributed to a particular individual, whether the comments are personal data about the speaker will depend on the capacity in which the speaker made the comments. That is to say, consider whether the individual is giving a personal opinion or is putting forward views on behalf of another individual, company or organisation (most commonly, the individual's employer).

Example: Where an individual attends a meeting in the capacity of an employee (for example, to discuss the provision of services by the company), if the employee expresses the views of the company, those views, when recorded in the minutes of the meeting, will not be personal data about the employee. The views will be information about the position of the company with regard to the service provision as expressed by its agent, the employee.

However, if allegations were made that the employee's representations failed to reflect the views of the organisation, information as to the representations made at the meeting could become personal data about the conduct of the employee.

The views of a company or organisation as expressed by its agent (either an employee or professional representative), are not personal data about the agent. The focus of the comments does not concern the employee's or agent's personal views but concerns the company's position.

7.2 Information about objects or things

When considering the 'focus' of information it may be helpful to consider whether the information is being processed to record something about an individual or to record information about an object.

Example: Information may be recorded about the operation of a piece of machinery (say, a biscuit-making machine). If the information is recorded to monitor the efficiency of the machine, it is unlikely to be personal data (however, see 8 below). However, if the information is recorded to monitor the productivity of the employee who operates the machine (and his annual bonus depends on achieving a certain level of productivity), the information about the operation of the machine will be personal data about the individual employee who operates it.

Whether information is linked to an individual, for example, to learn something about that individual, is the key factor in determining whether information about an object (for example, a biscuit-making machine) is personal data.

Also, if the information has potential to be used to learn something about an individual, it may be personal data as discussed below.

8 Processing which has an impact on individuals

Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?	
Yes	The data is 'personal data' for the purposes of the DPA.
No	The data is unlikely to be 'personal data'.

8.1 Can data about objects be personal data about an individual even though the data controller does not currently use such data to learn, record or determine something about that individual?

Even though the data is not usually processed by the data controller to provide information about an individual, if there is a reasonable chance that the data will be processed for that purpose, the data will be personal data.

Example: A taxi firm may record the movements of the taxis in its fleet by using vehicle tracking devices. The data is used by the firm to help provide the taxi service in that the control centre will know where all the taxis are at any one time and will therefore, on receiving a request for a taxi, be able to direct the nearest taxi to pick up the new passenger. The data is not intended to be used to inform the taxi firm as to the whereabouts of each individual taxi driver, but to plot the location of the fleet of taxis.

Even though the data was not intended to be used to record individual drivers' movements, the taxi control staff will usually know which driver is driving which taxi at any particular time and the data could therefore be used, without any adjustment, to locate a driver.

If family members needed to contact a taxi driver, they could ask one of the taxi control staff to use the taxi location data to provide the location. Consequently the taxi location data may be personal data about the taxi drivers.

If, as a matter of fact, data is occasionally processed to learn something about an individual, even though it was not the data controller's intention to process the data for this purpose, this data will be personal data as the processing does, or is likely to, impact on the individual.

Example: If we consider the taxi location data referred to in the example given above, if the control centre occasionally uses the taxi data to locate individual drivers, even though this was not the data controller's primary purpose for processing, the taxi location data will be personal data about the individual drivers.

When considering data about objects, if the data is processed to provide particular information about an individual (for example, information about a

biscuit-making machine is used to assess the productivity of the operator of the machine) the data will be personal data.

Where data about objects is not currently processed to provide particular information about an individual, but could be processed to provide information about an individual (for example, taxi location data) the data is likely to be personal data.

What is being considered here is whether the processing of the information has or could have a resulting impact upon the individual even though the content of the data is not directly about that individual, nor is there any intention to process the data for the purpose of determining or influencing the way that person is treated.

There will be circumstances where it remains uncertain whether particular data is personal data. Where this is the case we consider that, as a matter of good practice, you should still treat the information with care and, in particular, ensure it is held and disposed of securely.

Other issues concerning 'personal data' are addressed in the appendix attached to this guidance.

Appendix

Other issues concerning 'personal data'

A Personal data about more than one individual

Inevitably, because man is a social animal, a record which is mainly about one individual, and therefore personal data about that individual, will often contain personal information about another person, a partner, child, relative or friend. The DPA contains provisions which address the implications of this when responding to a subject access request[10].

There are circumstances where the same information is personal data about two or more individuals. This may be due to one of three factors:

(i) the content of the information is about two or more individuals;

Example: Consider the record of the arrest of an individual by a policeman. Where the individual arrested, or the arresting policeman, records an account of the circumstances of the arrest, if the record is held as data subject to the DPA, it will be personal data of both individuals.

There is no sensible way of separating the account of the direct interaction between the two individuals involved into personal information about each one separately. Indeed, the precise nature of the interaction leading to the arrest and its immediate consequences is a crucial part of the record.

(ii) the content of the information is about one individual but it is processed in order to learn/record/decide something about another individual;

Example: For each child attending a particular school, the school records emergency contact details identifying the name, address and phone number of the adult to be contacted should the child have an accident. The emergency contact information will be personal data about the adult (in that the content of the information comprises their name and contact details). The information will also be personal data about the child as the purpose of holding the information is to contact the child's responsible adult in the event of an emergency.

(iii) the personal information about one individual is personal data affecting another individual.

Example: An investigation is carried out into allegations made by an employee of bullying by a manager. In the course of the investigation other

[10] Section 7 DPA 1998

employees are asked about their dealings with the employee and the manager concerned. In these circumstances, the views of the employees who have been interviewed are likely to be personal data about both the complainant and the subject of the complaint and will also be personal data about the interviewee.

B Personal data in complaint files

There has been some confusion about whether the records associated with complaints can be personal data about individuals. Records relating to the consideration and investigation of complaints can be personal data about the person making the complaint, but this will depend on the circumstances.

Example: Where a newspaper complains that a government department has failed in its obligation to disclose information under the Freedom of Information Act 2000, the case file is unlikely to be personal data because the newspaper is not an individual. However, the complaint case file will almost certainly contain personal information identifying the journalist making the request on behalf of the newspaper and department officials dealing with the request.

It is possible that a case file could be personal data if, for example, it was about a particular official or Minister. If the request for information directly related to, or concerned, the conduct or activities of a particular Minister or other official, much if not all of the complaint case file is likely to be personal data about that Minister or official.

Example: Where an individual complains that a government department has not responded properly to a Freedom of Information request, and that therefore the individual's right to receive the requested information has been breached, the case file is likely to be personal data relating to the individual complainant.

Where a business requests a DPA assessment of the activities of another business, as they are entitled to do, the case file is unlikely to be personal data.

Example: Where an individual's complaint that a particular company has been fly-tipping prompts an investigation into the alleged incidents, the case file will contain information about the investigation and the case file will not be personal data about the individual complainant.

However, where an individual complains that a police force has not responded properly to a subject access request made under section 7 of the DPA, then the case file will be personal data relating to that individual.

Even in circumstances where the bulk of a case file is personal data about the individual complainant, it is likely to contain some personal information about

other individuals. It may well also contain information which is not, in itself, personal data, for example, if it includes details of policies and procedures relevant to the case.

C Information 'anonymised' for the purposes of the Directive

Article 1 of the Directive states that "personal data means any information relating to an identified or identifiable natural person." Recital 26 of the Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or any other person". This means that where, though it is conceivable that someone could identify a particular individual or individuals if they devoted sufficient effort and resources to the task, it is unlikely that anyone will do so then the individual(s) are not "identifiable" for the purposes of the Directive.

Data may be held as personal data by one organisation, because they can link the data to living identifiable individuals. The same data may be held by another organisation that is unable to link the data concerned to individuals. The question arises, therefore, whether the latter organisation holds personal data because the data, in the hands of another organisation, are linked to identifiable individuals.

The pragmatic line taken by the Article 29 Working Group is that where an organisation holds records which it cannot link, nor is ever likely to be able to link, to particular individuals, the records it holds will not be personal data. This will only be the case where it is unlikely that anyone else to whom the records may be released will be able to make such links. This will remain the case even if there is one organisation that would be able to make such a link as long as that organisation will not release information enabling such links to be made and adopts appropriate security. Where there is no likelihood of records being linked to individuals there is no real risk of any impact on those individuals. Therefore, where researchers hold samples of 'anonymised' individual census records released by the Office of National Statistics they will not be processing personal data even though the ONS may be able to link records to particular individuals.

There will be circumstances in which an organisation holds records relating to individuals where the obvious identifiers have been removed but where there is a need to be able to initiate contact with particular individuals if necessary.

Example: An EU based company carries out pharmaceutical research on identifiable individuals. They remove the obvious identifiers from the individual records (name, address etc) and key code them (that is they assign a unique code such as KLPR767805 to each individual record). They then release the 'anonymised' individual records to another pharmaceutical company which will use them for further research. In the event that the second company identifies that a particular individual might be at risk because of the combination of

their illness and the drugs they are using, the second company can alert the first company, 'identifying' the individual in question by means of the code. The first company can then contact the individual. The key question is whether the second company holds the records in question as personal data.

The second company is able to isolate particular records where the medical histories and current medication give cause for concern and 'identify' them by means of the codes. Unless there are exceptional circumstances, for example where an individual has a very rare condition and there has been publicity in the press which named them, it is unlikely that the second company will ever find out the name and address or other information which would enable them to physically find the individual in question. However, by alerting the first company to their concerns they do cause the individual to be contacted and thus their processing has a clear effect on the individual. Nevertheless, because they do not contact the individual themselves and because they have no interest in the individuals themselves, merely in ensuring that where records give cause for concern the individual is contacted, we consider that for all practical purposes they do not hold the key coded records as personal data. A significant consideration here is that as long as the first company have appropriate security in place there is little or no chance that any other person who might have access to the coded records would be able to link an individual by name and or address to a particular record. In such circumstances the chances of an individual suffering detriment are negligible.

D Disclosing information which could be linked to identifiable individuals

A question faced by many organisations, particularly those responding to Freedom of Information requests, is whether, in disclosing information that does not directly identify individuals, they are nevertheless disclosing personal data if there is a reasonable chance that those who may receive the data will be able to identify particular individuals.

Example: An organisation receives a Freedom on Information request for the full home addresses of its staff but without staff names attached.

Organisations need to consider whether, by releasing the addresses, they will have released personal data. The DPA refers to data which relate to a living individual who can be identified from that data or from that data and other information in the possession of, or likely to come into the possession of, the data controller. This emphasis on identification of individuals by "the data controller" might suggest that, even if there is a reasonable chance that someone other than the recipient of the address information might be able to link particular addresses to specific staff members, the data controller has not released personal data merely by releasing the addresses to the particular FOI applicant. However, the definition of personal data in the Directive suggests otherwise.

The Directive provides that "personal data shall mean any information relating to an identified or identifiable natural person ...; an identifiable person is one who can be identified, directly or indirectly...".

This definition would suggest that an organisation would be disclosing personal data where it releases information which can be linked to particular individuals. Taking into account the purpose of the Directive this seems a sensible view. It is a view which the Information Tribunal took when deciding whether a local authority should release the addresses of empty properties. The Tribunal held that releasing such addresses would involve releasing personal data where the properties were owned by individuals.

16.8.07

BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Document Retention

EU Data Protection

Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements

FRED H. CATE AND MARGARET P. EISENHAUER

Fred H. Cate is a Distinguished Professor of Law, Adjunct Professor of Informatics, and Director of the Center for Applied Cybersecurity Research at Indiana University, and Senior Policy Advisor in the Center for Information Policy Leadership at Hunton & Williams LLP.

Margaret P. Eisenhauer is the founder of Privacy & Information Management Services-Margaret P. Eisenhauer, P.C. law firm, a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board.

These materials have been prepared for informational purposes only and are not legal advice. Additionally, the views expressed herein are those of the authors personally, and do not necessarily reflect the views of their clients, employers or associates.

Companies in the United States are routinely required to retain and disclose internal records in the course of civil litigation. Among the most familiar of these requirements are the obligations to protect evidence relevant to pending or reasonably foreseeable litigation and to produce documents sought under a subpoena or court order.

For documents stored outside the United States, retention and production requirements often conflict directly with international data protection laws. As multinational companies link their affiliates on global networks and leverage consolidated data processing hubs, corporate documents are increasingly located in other countries. The implications for companies facing complex discovery in connection with U.S.-based litigation can be profound.

U.S. Document Production Requirements

Rule 34 of the U.S. Federal Rules of Civil Procedure governs the production of documents in civil litigation before the federal courts. Under Rule 34, companies have a legal duty to retain *all documents* that may be relevant to pending and reasonably foreseeable litiga-

 ISSN 1538-3423

tion. During the discovery process, companies are obligated to search and produce all relevant records.

The failure to preserve documents for the other party's use as evidence is spoliation. The corporate scandals involving Enron and Arthur Andersen both involved charges of spoliation. The consequences for spoliation may include adverse rulings in the litigation as well as criminal sanctions and independent tort claims.

Under Rule 34, the duty to preserve documents applies irrespective of the format in which they are maintained. The Rule was amended in 2006 expressly to state that the term "documents" includes all types of electronically stored information.[1] The amendment confirmed that "discovery of electronically stored information stands on equal footing with discovery of paper documents" and clarified that "a Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information."[2]

Given the consequences of spoliation, U.S. companies are wisely focused on records management and preservation. Many companies have implemented systems that automatically scan all electronic records (including e-mails) and copy those records that may be relevant to possible future litigation. These systems are generally invisible to users, who may not realize that their documents are being scanned and copied for future document production purposes. Multinational companies using these systems must also consider the conflicts that exist between the Rules of Civil Procedure and international data protection laws.

European Data Protection Laws

European data protection laws codify the concept of privacy as a fundamental human right. In accordance with the European Union Data Protection Directive,[3] each member state has enacted a national data protection law governing the "processing of personal data."

The scope of the European data protection laws cannot be understated. "Processing" is broadly defined as "any operation or set of operations," whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[4] "Personal data" are defined equally broadly as "any information relating to an identified or identifiable natural person."[5]

The general rule in Europe is that companies must collect only the personal data they need to fulfill a specific legitimate purpose, then use, disclose and retain the data only as needed for that purpose. The use of business records that reveal personal data (such as e-mails) in the course of litigation is a secondary use, which requires (at minimum) the consent of the data subject. But the mere retention of the records containing personal data in anticipation of a discovery request would itself violate this general rule.

European data protection laws guarantee individuals access to and the opportunity to correct and request deletion of information held about them. Data subjects are also entitled to object to the processing of their personal data, and they must be offered the opportunity to have their personal data erased before they are disclosed to third parties or used for secondary purposes. To enable individuals to understand how their data is used and exercise their rights, the laws require companies to provide detailed privacy notices.

European data protection laws also generally prohibit the transfer of personal data to countries outside of Europe that do not provide an adequate level of protection. As discussed below, the data transfer prohibition is subject to some exceptions. Unfortunately, these exceptions are interpreted very narrowly by the European regulatory community.

Finally, the data protection laws establish independent data protection authorities to supervise compliance efforts and hear data subject complaints. These authorities have the power to investigate data processing activities and to order the cessation of processing and the erasure of personal data. The authorities meet collectively as a group created by Article 29 of the Directive to issue guidance on the application of the Directive.[6]

Across Europe, the data protection authorities take their oversight roles very seriously. They routinely conduct investigations, bring enforcement actions, levy fines, and, in some cases, even seek criminal penalties for non-compliance with the data protection laws. Additionally, while the threat of large fines is daunting, companies also risk burdensome investigations and the possibility that their data transfers may be disrupted. This latter risk is very real; transfers of even innocuous employee data from Europe have been blocked as a result of legal violations. [7]

Processing of Personal Information for U.S. Litigation

While the restrictions on transborder data flows are the focal point of many U.S. company concerns about data protection law compliance, it is important to remember that these restrictions only come into play if the personal data have otherwise been lawfully processed within Europe. However, the mere retention and searching of records containing personal data of EU nationals (such as e-mails) for Rule 34 compliance purposes will likely violate EU data protection laws, even if the data never leave Europe.

Of all of the privacy interests implicated by the Rule 34 production requirements, perhaps the most complex are those of the employees, whose documents and e-mails are subject to retention and disclosure. As a preliminary matter, the data protection authorities regard virtually all data about employees as personal data, subject to the data protection laws.[8] Almost all business

[1] *Report of the Judicial Conference Committee on the Rules of Practice and Procedure* 71-72 (Sept. 2005)

[2] Id. at 72

[3] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281)

[4] Id. art. 2(b)

[5] Id. art 2(a)

[6] This group is referred to as the Article 29 Working Party.

[7] See, *e.g.*, Jennifer L. Kraus, On the Regulation of Personal Data Flows in Europe and the United States, 1993 *Colum. Bus. L. Rev.* 59, 71 (1993)

[8] Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, Sept. 13, 2001 (5062/01/EN/Final WP 48)

  PVLR ISSN 1538-3423

records contain some personal information, such as the name of the individual that created the document or the e-mail addresses of the sender and recipients.

The Article 29 Working Party has developed an extensive body of interpretation concerning the protection of employees' personal data. Although the analysis focuses on employee data, it should be remembered that the same legal requirements will apply to the data of other individuals contained in the company's records.

European regulators have repeatedly stressed that employers can only process personal data "lawfully," in accordance with established data protection principles, including:

- Finality: personal data may be processed only for specific, stated purposes and may not be processed for any other incompatible purpose.
- Legitimacy: personal data may only be processed for "legitimate" purposes as set forth in the Data Protection Directive.
- Proportionality: processing of personal data may not be excessive in relation to the purposes for which it was collected.
- Transparency: employers must notify employees of the data it is collecting about them, must give employees access to such data, and state the purposes for which the data are processed.[9]

Compliance with these principles trumps any employer interest or claim of necessity:

> The legitimate interests of the employer justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in Directive 95/46/EC. *Workers can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms.*[10]

Using the principles as a starting point, employers may process data concerning their employees for lawful and legitimate purposes with "unambiguous consent" or if the processing is "necessary." [11] Consent and necessity provide the only legitimate basis for data processing. Unfortunately, neither consent nor necessity support the kinds of processing required for Rule 34 compliance, and the data protection authorities generally believe that any inspection of employee communications, such as e-mail, violates the principles stated above.

Consent is problematic as a basis for processing for document production. To be valid, consent must be both freely given and capable of being revoked. The Working Party makes this point repeatedly: "If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice."[12]

From a Rule 34-standpoint, however, companies cannot permit employees to opt-out of having their documents examined in connection with document production requests. Companies cannot rely on consent as the basis for its discovery and production requirements.

Employers must therefore rely on the "necessity" of the processing for document production efforts. This approach is problematic as well, however, because the Article 29 Working Party has concluded that there are only three types of really "necessary" processing:

- Processing required for the employer to perform its contractual obligations vis-a-vis an employee (*e.g.*, processing an employee's salary data for payroll);
- Processing required for the employer to protect an employee's vital interests (*e.g.*, to protect the employee against particular hazards at the workplace); and
- Processing required for an employer to comply with its domestic legal obligations in Europe (*e.g.*, processing an employer's data for the purpose of calculating the withholding tax).[13]

The Working Party does not agree that compliance with extra-territorial legal requirements is "necessary" to justify processing of employee data in Europe. This conclusion was forcefully demonstrated in the data protection authority response to U.S. company establishment of whistleblower hotlines in Europe as required by Section 301 of the Sarbanes-Oxley Act.[14]

Moreover, analysis of employee e-mails—an essential part of the discovery process—is viewed with exceptional hostility. Where employers examine employee e-mails in connection with specific employee wrongdoing, they have often faced legal sanction. This is most vividly demonstrated in *Societe Nikon France v. M. Onof*.[15] There the French high court held that an employer had no legal right to intercept and read employees' e-mails and other documents, even if the employer supplied the computer and expressly provided that employees were not to use their computers for personal uses. The court stated that monitoring personal messages violates this fundamental freedom even if the employer prohibits the usage of the computer for non-professional purposes.[16]

Similarly, in May 2006, the French high court ruled that, absent exceptional circumstances, an employer has no right to invade the personal privacy of employees in their workplace computers.[17] In this case, a company found "erotic photos" on a worker's desk; as a result, the company searched the employee's work-issued computer, discovered that he had downloaded pornographic images and fired him. Although lower French courts upheld the search and firing, the high court disagreed, noting that the presence of pornography on the

[9] Id. at 3
[10] Id. at 28 (emphasis added)
[11] Id. at 15-16
[12] Id. at 23
[13] Id. at 15
[14] See Article 29 Data Protection Working Party, *Opinion 1/2006 on the Application of E.U. Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime*, Feb. 1, 2006 (00195/06EN WP117)
[15] Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291.
[16] See Yohei Suda, "Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States," 4 *Wash. U. Global Stud. L. Rev.* 209 (2005), 253-256.
[17] *Philippe K. v Cathnet-Science*, Cour de Cassation, Chambre Sociale, Arret No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017, 5/17/05. Reported in the BNA *Privacy Law Watch* (June 6, 2005).

computer did not present the type of risk that could justify an unauthorized search of the computer.[18]

The French position is not unique. The Greek data protection authority held in 2004 that even a technological "intervention" (such as automated scanning) by an employer of employee e-mails is illegal unless the employee is informed of the intervention and given a "technical means of using special software to protect the secrecy of his own communication."[19] In Italy, employers are also prohibited from monitoring e-mails; the Italian Supreme Court has held that "an employer can only carry out such monitoring if it is aimed at ascertaining unlawful behavior on the part of the employee and provided it has reached an agreement with the local union or has authorization from the local labor office."[20]

Given the state of the law around employee e-mails, it is difficult to imagine how a company could justify examining e-mails or computer files merely in anticipation of U.S. litigation—even if Rule 34 requires precisely that.

Indeed, in the one case that has considered the conflict between EU privacy laws and U.S. production requirements, the privacy right, as expected, triumphed. In 1995, the German government intervened in a U.S. state court civil case to object to the production of Volkswagen's printed corporate telephone directory. Based on that intervention and expert testimony about the scope and burden of German privacy laws, the Texas Supreme Court concluded that the "corporate phone book should not be produced in contravention of German law."[21]

International Transfers of Personal Information

Even if personal data are lawfully obtained and processed, they may not be transferred outside of the EU unless the recipient country offers adequate protection or an exception to the transborder transfer restriction applies. Since the United States has not been declared adequate, data transfers from the EU to the United States can only occur if:

- The recipient is in the U.S. Safe Harbor;[22]
- The transfer is authorized using an approved model contract; [23] or
- Another exception to the data transfer restrictions applies.[24]

Unfortunately, none of these mechanisms provide cover for U.S. companies that need to process and transfer business records containing personal information (especially employee information) to the U.S. for document production purposes.

Under the Safe Harbor agreement, U.S. entities self-certify that they are abiding by the Safe Harbor Principles. These companies may believe that the Safe Harbor provides a mechanism for processing and transferring personal data in the context of U.S.-based document production efforts because the Principles state:

> [a]dherence to these Principles may be limited: . . . by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization. . . .[25]

This interpretation is extremely risky, however, for two reasons.

First, the Safe Harbor provides a legal basis only for exporting personal data from the EU—it does not authorize any additional processing within Europe, nor does it broaden the ability of the organization to further process the data once in the United States. EU and U.S. negotiators explicitly agreed that "where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes," the "U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes."[26]

Second, despite the general principle that Safe Harbor enforcement is the responsibility of U.S. regulators, the European data protection authorities retained jurisdiction to handle data protection violations concerning employee data.[27] Accordingly, the strict EU interpretations of the exceptions will prevail.

The model contracts are no better than Safe Harbor. Under the model contracts, the data exporter and the data importer agree to comply with applicable EU laws or similar data protection principles, thus limiting the U.S. company's ability to include the EU data in U.S. discovery and production initiatives. And, again, the data protection authorities have jurisdiction to address any perceived violations.

Neither the Safe Harbor nor the model contracts provide any resolution of the conflicts created by the EU data protection laws when employee data or other personal information is processed in the context of U.S.-based document production efforts. Conversely, companies using these data transfer constructs may have even greater risk. By bringing personal data to the U.S. pursuant to Safe Harbor or a model contract, they are in the precarious position of having data in the U.S. that is clearly subject to the Rule 34 requirements but without the authority to process the data as needed to meet those requirements.

Article 26 of the EU Data Protection Directive contains exceptions to the general prohibition on transborder data flows. Under Article 26(1)(c), personal data may be transferred as "for the establishment, exercise

[18] Id .

[19] *Eighth Annual Report of the Article 29 Working Party on Data Protection* (2005) at 44 (citing Decision 61/2004)

[20] "Monitoring Employees E-Mail and Internet Usage in Europe," *Internet Law-Business-e-Commerce*, May 1, 2005.

[21] *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900 (Tex. 1995)

[22] Commission Decision 2000/520/EC of 26.7.2000 - O. J. L 215/7 of 25.8.2000

[23] Commission Decision 2001/497/EC and Commission Decision C(2004)5271

[24] *E.g.*, a derogation under Article 26(1) of the E.U. Data Protection Directive. Companies can also seek specific permission from the applicable data protection authorities for the transfer, but the operational difficulties of obtaining such permission (and the low likelihood that it would be granted) render this approach of almost non-existent practical value.

[25] U.S. Department Of Commerce, Safe Harbor Privacy Principles (July 21, 2000), available at <http://op.bna.com/pl.nsf/r?Open=byul-6y2qtw>.

[26] Safe Harbor, FAQ 9 (Human Resources)

[27] Id.

  PVLR ISSN 1538-3423

or defence of legal claims." While this derogation seems to provide exactly what U.S. companies need, it cannot be used to support the document discovery processes necessary to comply with Rule 34 either.

All of the Article 26(1) derogations are interpreted very narrowly by the European regulatory community, and 26(1)(c) is no exception. [28] According to a Working Party example, "the parent company of a multinational group, established in a third country," that was being sued by one of its own European employees could transfer "certain data" relating to that employee from its European subsidiary if those data were necessary for its defense. But "this exception cannot be used to justify the transfer of all the employee files to the group's parent company on the grounds of the possibility that such legal proceedings might be brought one day."[29]

Moreover, the Working Party has limited the application of this exception to those cases in which "the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" Convention) and of 25 October 1980 ("Access to Justice" Convention)" have been complied with.[30] The U.S. is not a signatory to the Access to Justice Convention and U.S. law does not require courts to follow the procedures of the Hague Convention on the Taking of Evidence. As a result, the Article 26(1)(c) exception appears inapplicable to U.S. document production requests.

Additionally, even if the derogation did apply, it would not exempt the company from otherwise complying with all of the provisions of the data protection laws (such as limits on e-mail scanning), and it can be trumped if the transfer, in the eyes of the relevant authority, would violate the fundamental rights of the data subject. The Working Party's language is stark:

> It should also be noted, however, that the provisions of the Directive relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive. As explicitly mentioned in Article 25(1), these provisions apply "without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive". This means that regardless of the provisions relied upon for the purpose of data transfer to a third country, other relevant provisions of the Directive need to be respected.[31]

Conclusion

The Rule 34 requirements pose almost insurmountable risks for companies with operations in Europe or other countries with EU-style data protection laws. These laws require both government permission and compelling justification before even the most innocuous personal data can be collected, retained, exported from the jurisdiction, or disclosed to a third party.

The conflicts between U.S. discovery requirements and international data protection laws will only become more pronounced, given the increasing use of consolidated data systems and the expanding reach of U.S. document production orders. Unfortunately, these conflicts likely cannot be resolved by companies due to the vast number of data protection authorities and lack of support for U.S.-government mandated processing generally.

Given the current attitudes of EU data protection authorities around employee-data processing generally (and employee monitoring in particular), it is unlikely that support for the types of vast data-mining and analysis required by U.S. discovery orders will be found. This likelihood is reduced even further by the current controversies between Europe and the United States over the transfer of air passenger name records or the SWIFT international financial data.

Europe is not alone. To date, EU-style laws have been enacted in many other countries, including Argentina, Australia, Canada, Hong Kong, Japan, New Zealand, and Russia. To be certain, not all of these laws are as complex or as zealously enforced as their EU models, but many of the substantive requirements are similar if not identical.

Ultimately, an accommodation, if not a solution, will have to be found. Judging from the experience with the Safe Harbor and passenger information agreements, that accommodation will result not by pressuring companies caught between two sets of conflicting legal requirements, but through long, careful, detailed negotiations between governments.

---

[28] *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*

[29] Id. at 15

[30] Id. at 15

[31] Id. at 8

Law.com's In-House Counsel

European Data Privacy Laws Pose E-Discovery Problems

Michael B. de Leeuw and Philip A. Wellner
New York Law Journal
May 21, 2008

While the collection, review and production of e-mails and other electronic documents have become routine for U.S. companies involved in civil litigation, internal investigations, and various other legal matters, there is an increasing number of cases that involve foreign or multinational clients, and the collection and production of electronic documents from these clients can be anything but routine.

Clients with operations in the European Union pose a particular problem for electronic discovery because of the strict data privacy laws in most European jurisdictions, which regulate the processing of personal data and its export from the EU. These laws create a significant tension between a foreign or multinational company's obligations to produce documents for U.S. legal matters and its compliance with European law.

This is an evolving area of the law, and it is imperative that U.S. lawyers become familiar with the data privacy issue and work closely with their clients to address them before a single document gets reviewed.

THE SOURCE OF EU DATA PRIVACY

The main source of European data privacy law, Directive 95/46/EC, was adopted by the European Commission on Oct. 24, 1995. Its stated purpose was to harmonize the levels of data privacy protection in member states in order to remove obstacles to the free flow of information within the Community while "protect[ing] fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law." [¶ 10].

Under the directive, these rights are protected even when the electronic data has been transmitted outside the EU: "the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive." [¶ 20].

The directive was adopted through national legislation throughout the EU.[FOOTNOTE 1] Each country's implementing legislation must adhere to the directive, but variations exist in the text and especially in the enforcement of the laws and potential penalties.

It is sobering to note, for example, that the French data protection authority levied a 30,000 euro fine against Tyco Healthcare France, a first-time violator after an on-site investigation found criminal violations of France's data protection act.[FOOTNOTE 2] It is important, therefore, to learn the specific rules and practices of the European country in which your client has operations.

THE DIRECTIVE IN OPERATION

The directive operates in two ways: It regulates the "processing" of personal data and the "transport" or "export" of data outside of the EU.

Its treatment of processing of personal data is important because of the very broad scope of activities that are considered "processing" and are therefore within the scope of the directive. The directive's treatment of data transport is equally important for attorneys in the U.S. because it determines the availability of data for compliance with the discovery process.

The directive defines "personal data" as "any information relating to an identified or identifiable natural person."[FOOTNOTE 3] Under this definition, personal data may often be contained within documents that a company or its legal counsel collects during the discovery process. If a document identifies a particular individual, whether by name, e-mail address, or some other description, so long as it "relates to" the individual, it falls within the scope of the data privacy laws. For example, if the data is about an individual, is linked to an individual (e.g., salary information), is to be used for actions relating to an individual, or is of biographical significance, then it qualifies. [FOOTNOTE 4]

"Processing" is similarly broad. The term encompasses "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" of personal data, whether done through an automated process or manually.[FOOTNOTE 5] "Processing" therefore, covers virtually any action that a U.S. litigator would take in the course of reviewing or producing e-mails, electronic documents, or even hard copy documents that have been scanned electronically.[FOOTNOTE 6]

Chapter IV of the directive governs the transfer of personal data to countries outside of the EU. Its principal provision is that personal data may not be transferred to countries that do not afford an adequate level of protection, i.e., the same level of protection provided by the directive and its implementing legislation. To date, the Commission has only designated a handful of non-EU countries as offering sufficient protection: Switzerland, Canada, Argentina, Guernsey and the Isle of Man.

Notably, of course, the U.S. is not on this list. And while the U.S. Department of Commerce's Safe Harbor Privacy Principles has been deemed by the Commission to offer the required level of protection,[FOOTNOTE 7] the Department of Commerce program does not control, and is, in fact, incompatible with, typical discovery in the United States.

Companies within the EU are permitted to collect and process personal data for a variety of specifically enumerated purposes, and, in limited circumstances, they may also transmit the data to non-EU countries that do not offer adequate protection. Only one of these exceptions offers language helpful on its face to attorneys in the United States.

The directive[FOOTNOTE 8] carves out an exception that permits the processing and the export of personal data where it is "necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)."[FOOTNOTE 9] This provision would seemingly allow companies to review and produce documents pursuant to discovery proceedings in the United States. Unfortunately, this exception is much narrower than it appears. Indeed, complying with legal obligations in the United States may not fall within the scope of this exception.

WORKING PARTY OPINION IS NO HELP

After passage of the directive, the European Commission established the Article 29 Data Protection Working Party, which consists of representatives of each of the member states' data protection authorities plus a representative of the Commission.[FOOTNOTE 10] Though the Working Party's status is advisory, it is specifically charged with giving opinions on the adequacy of the level of data privacy protection in non-EU countries and with making recommendations regarding data privacy protection.[FOOTNOTE 11]

The Working Party adopts several opinions each year that are designed to guide the interpretation of data protection principles enshrined in the directive and member state laws.[FOOTNOTE 12] One of these opinions undermines reliance on the "legal proceedings" exception for those of us who need to export data to the United States.

In 2006, the Working Party addressed the subject of data processing by companies that needed to comply with Section 301 of the Sarbanes-Oxley Act. One of the opinion's conclusions was that compliance with extra-territorial legal requirements, i.e., those imposed by U.S. law, does not justify the processing of employee data beyond what is otherwise permitted by the directive.[FOOTNOTE 13]

The Working Party's justification for this opinion was that "any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC."[FOOTNOTE 14] The opinion must be read, therefore, as precluding the use of the "legal proceedings" exception to justify transporting data to the United States to satisfy discovery obligations. Commentators have interpreted the opinion in this manner,[FOOTNOTE 15] and thus far there is no authority to the contrary.

OTHER EXPORT METHODS ARE RISKY

Theoretically, there are three other methods for exporting electronic data to the United States, but as some commentators have pointed out each is fraught with significant risk and potential conflict with U.S. discovery procedures.[FOOTNOTE 16]

The first method is to get the consent of each individual whose data is to be transferred. Apart from the potential logistical problems of seeking the consent of potentially hundreds of e-mail senders and recipients, document authors, and others whose data is contained in these documents, this option is not practical because, in order for each individual's consent to be valid under the EU laws, the consent must be revocable at any time. This requirement cannot be reconciled with Federal Rule of Civil Procedure 34, under which employees cannot opt out of having their documents examined as part of discovery proceedings.[FOOTNOTE 17]

The second and third methods are equally problematic. The second involves using a model contract, promulgated by the Working Party, through which the company agrees to comply with EU data protection rules in the export of the data. The third method involves certification of the company under the Safe Harbor Program administered by the U.S. Department of Commerce.

The Safe Harbor is not a practical solution for the discovery process, because it only permits the export of the data,

not any further processing. The prohibition on further processing would make the data unusable for discovery, since any document production and review activities that take place in the United States are likely to fall within the scope of the "processing."

At the same time, use of the Safe Harbor to bring the data to this country would make the data subject to subpoena. If subpoenaed, the company would then face the uncomfortable dilemma of violating either U.S. or EU law by producing or withholding the data.

The model contracts are similarly unhelpful. While they permit the data to be processed outside the EU for the purposes stated in the contract, they require the company to continue to abide by the EU data privacy laws in a manner incompatible with U.S. civil discovery[FOOTNOTE 18] by limiting their availability for document review and production.

Of further concern is the fact that under both the model contracts and the Safe Harbor, the national data privacy authorities in the EU retain jurisdiction to prosecute any violations of national data privacy laws.[FOOTNOTE 19] In the UK, for instance, violations of the Data Protection Act are investigated by the Information Commissioner's Office, which issues enforcement notices that require the company to certify compliance with the Act.[FOOTNOTE 20] Persistent violators who fail to comply with an enforcement notice are subject to criminal penalties, which can range from 5,000 pounds per violation to potentially unlimited fines.[FOOTNOTE 21]

The model contracts also require that the individual to whom the data relates be included as a third-party beneficiary to the contract, which gives them a cause of action against both the exporter and importer of the data for any breaches of the agreement.[FOOTNOTE 22]

AT THE MOMENT, NO EASY ANSWER

At this stage, there is no simple method by which EU documents containing personal data can be collected and transported to the United States for the purpose of review and production. And there is no general procedure for requesting permission from EU data privacy authorities to export such data. While we can hope that this will change in the near future, the smooth operation of civil litigation in the U.S. is probably not high on the priority list of our friends in Europe.

For now, the most reliable approach is to seek production of the documents through the country's courts. Pursuant to Rule 28, a party seeking the production of documents should obtain a letter of request under the Hague Evidence Convention from a district court, which will then be transmitted to the appropriate national court in the EU.[FOOTNOTE 23] Once production of documents is ordered by the European Court, the legal obligation that the party holding the documents must satisfy is no longer extra-territorial, and the legal proceedings exception will presumably be satisfied and permit the documents to be transferred.

Unfortunately, this process can take a substantial amount of time; it is common for execution of letters of request to take six to 12 months or more.[FOOTNOTE 24] Though this approach may seem burdensome, it avoids the substantial risk of running afoul of EU data privacy laws, a risk that multinational companies should not take lightly.

An additional approach, which has logical appeal but has not yet been tested in court, is to review the data in Europe under the directive's exception that permits processing (but not export) where "processing is necessary for the purposes of the legitimate interests pursued by the [company] or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests ... of the data subject[.]"[FOOTNOTE 25]

Under this exception, the Working Party has permitted companies to process data in Europe pursuant to obligations imposed by the Sarbanes-Oxley Act.[FOOTNOTE 26] It is important to note, however, that the Working Party engaged in a fact-specific balancing test of the interests of the company and the individual before reaching this conclusion, and required a series of safeguards to be imposed on the processing. But assuming that sufficient safeguards are put into place this method should allow a company to conduct a thorough review of its material, remove the vestiges of personal data, and then export the remaining data to the U.S. where it can be produced or otherwise used.

The downsides to this process are that it has not been ruled on by a court or the Working Party, and the costs associated with reviewing documents in Europe can be considerable.

The key is to be aware of the data privacy laws and develop a plan with your client that is as consistent as possible with obligations under U.S. and EU law.

Michael B. de Leeuw is a litigation partner, and Philip A. Wellner is an antitrust associate, with Fried, Frank, Harris, Shriver & Jacobson.

:::::FOOTNOTES:::::

FN1 See European Commission, Justice and Home Affairs -- Data Protection, Status of Implementation of Directive 95/46/EC, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

FN2 See Commission Nationale de L'informatique et des Libertés, Délibération n°2006-281 du 14 décembre 2006 sanctionnant la société Tyco Healthcare France, http://www.cnil.fr/index.php?id=2207.

FN3 Council Directive 95/46/EC, art. 2(a), O.J. (L281).

FN4 See, e.g., UK Information Commissioner's Office, Data Protection Technical Guidance: Determining What Is Personal Data, at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf.

FN5 Council Directive 95/46/EC, art. 2(b), O.J. (L281).

FN6 Id. The definition of "processing" likely includes the collection and sorting of hard copy documents -- depending on their contents -- that are never processed electronically. Though no authority has been found addressing this

question, since collection is considered to be a form of processing, any hard copy documents that contain personal data should be treated as falling within the scope of the protections discussed by this article.

FN7 See European Commission, Justice and Home Affairs -- Data Protection, Adequacy of Protection of Personal Data in Third Countries, at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

FN8 See Council Directive 95/46/EC, art. 26, para. 1(d), O.J. (L281).

FN9 See, e.g., UK Data Protection Act of 1998, 1998 Chapter 29, Schedule 4(5)(a).

FN10 See Council Directive 95/46/EC, art. 29, O.J. (L281).

FN11 See Council Directive 95/46/EC, art. 30, para. 3, O.J. (L281).

FN12 See European Commission, Justice and Home Affairs -- Data Protection, Documents Adopted by the Data Protection Working Party, at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm.

FN13 See Article 29 Data Protection Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime, 00195/06/EN, at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf, p. 8.

FN14 Id.

FN15 See generally Fred H. Cate and Margaret P. Eisenhauer, "Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements," PRIVACY & SECURITY LAW REPORT, BNA Inc., 2007.

FN16 Id.

FN17 Id.

FN18 Id.

FN19 Cate & Eisenhauer at 4.

FN20 Again, it is important to learn the specific enforcement rules of the country in which your client has data. As noted above, the French data protection authority imposed significant criminal penalties on Tyco Healthcare, a first-time offender.

FN21 UK Information Commissioner's Office, Criminal Offences, at http://www.ico.gov.uk/what_we_cover/data_protection/our_legal_powers/criminal_offences.aspx.

FN22 See, e.g., Miriam Wugmeister et al., "Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules," 38 GEO. J. INT'L L. 449, 459 (2007).

FN23 See, e.g., 6-28 Moore's Federal Practice §§28.11, 28.12.

FN24 6-28 Moore's Federal Practice §28.12.

FN25 Council Directive 95/46/EC, art. 7(f), O.J. (L281).

FN26 See Article 29 Data Protection Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime, 00195/06/EN, at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf, p. 8.

00195/06/EN

WP 117

Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

Adopted on 1 February 2006

TABLE OF CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,[1]

Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure, and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

This opinion provides guidance on how internal whistleblowing schemes can be implemented in compliance with the EU data protection rules enshrined in Directive 95/46/EC.[2]

The number of issues raised by the implementation of whistleblowing schemes in Europe in 2005, including data protection issues, has shown that the development of this practice in all EU countries can face substantial difficulties. These difficulties are largely owed to cultural differences, which themselves stem from social and/or historical reasons that can neither be denied nor ignored

The Working Party is aware that these difficulties are partly related to the breadth of the scope of issues which may be reported through internal whistleblowing schemes. It is also aware that whistleblowing schemes raise specific difficulties in some EU countries with regard to labour law aspects, and that work is ongoing on these issues which will require further attention. The Working Party also needs to take into account the fact that in some EU countries the functioning of whistleblowing schemes is provided for by law, while in the majority of EU countries no specific legislation or regulation exists on this issue.

As a result, the Working Party deems it premature to adopt a final opinion on whistleblowing in general at this stage. By adopting this opinion, it has decided to address those issues on which EU guidance is most urgently needed. Considering this, and for reasons mentioned in the document, this opinion is formally limited to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing mattrers, fight against bribery, banking and financial crime.

---

1 OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

2 In accordance with the specific mandate of the Working Party, this working document does not address other legal difficulties raised by whistleblowing schemes, in particular in relation to labour law and criminal law.

The Working Party adopted this opinion on the clear understanding that it needs to further reflect on the possible compatibility of EU data protection rules with internal whistleblowing schemes in other fields than the ones just mentioned, such as human resources, workers' health and safety, environmental damage or threats, and commission of offences. It will pursue its analysis over the coming months to determine whether EU guidance is also needed on these issues, in which case the principles developed in this document might be supplemented or adapted in a subsequent document.

II. JUSTIFICATION FOR THE LIMITED SCOPE OF THE OPINION

The Sarbanes-Oxley Act (SOX) was adopted by the US Congress in 2002 following various corporate financial scandals.

SOX requires publicly held US companies and their EU-based affiliates, as well as non-US companies, listed in one of the US stock markets to establish, within their audit committee, *"procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters"*.[3] In addition, Section 806 of SOX lays down provision aimed at ensuring the protection for employees of publicly traded companies who provide evidence of fraud from retaliatory measures taken against them for making use of the reporting scheme.[4] The Securities and Exchange Commission (SEC) is the US authority in charge of monitoring the application of SOX.

These provisions are mirrored in the Nasdaq[5] and New York Stock Exchange (NYSE)[6] rules. If listed on either Nasdaq or NYSE, companies must certify their accounts to those markets yearly. This certification process implies that companies are in a position to assert that they comply with a number of rules, including whistleblowing rules.

Companies which fail to comply with these whistleblowing requirements are subject to heavy sanctions and penalties by Nasdaq, NYSE or the SEC. As a result of the uncertainty as to the compatibility of whistleblowing schemes with EU data protection rules, the companies concerned are facing risks of sanctions from EU data protection authorities if they fail to comply with EU data protection rules, on the one hand, and from US authorities if they fail to comply with US rules, on the other.

The applicability of some SOX provisions to European subsidiaries of US companies and to European companies listed in US stock markets is at present under judicial review in

---

3 Sarbanes-Oxley Act, Section 301(4).

4 Sarbanes-Oxley Act, Section 406, and, more particularly, regulations enacted by major US stock exchange institutions (NASDAQ, NYSE) also lay down that companies listed in those markets adopt "codes of ethics" applicable to senior financial officers and directors, concerning accounting, reporting and auditing matters, that should provide for enforcement mechanisms.

5 Rule 4350 (D) (3): "Audit Committee Responsibilities and Authority"

6 New York Stock Exchange (NYSE), Section 303A.06: "Audit Committee"

the United States.[7] Despite this relative uncertainty as to the applicability of all of the SOX provisions to companies established in Europe, companies which are subject to SOX on the basis of clear extraterritorial provisions in this Act also want to be in a position to comply with the specific whistleblowing provisions of SOX.

Due to the risk of sanctions facing EU companies, the WP29 has deemed it urgent to concentrate its analysis primarily on whistleblowing systems established for the reporting of potential breeches in accounting, internal accounting control and auditing matters, such as referred to in the Sarbanes-Oxley Act, and on related matters mentioned below. In so doing, the Working Party intends to contribute to the provision of legal certainty to companies which are subject both to EU data protection rules and to SOX.

III. PARTICULAR EMPHASIS PUT BY DATA PROTECTION RULES ON THE PROTECTION OF THE PERSON INCRIMINATED THROUGH A WHISTLEBLOWING SCHEME

Internal whistleblowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of companies. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel. It supplements the organisation's regular information and reporting channels, such as employee representatives, line management, quality control personnel or internal auditors who are employed precisely to report such misconducts. Whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management.

The Working Party stresses that whistleblowing schemes must be implemented in compliance with EU data protection rules. As a matter of fact, the implementation of whistleblowing schemes will in the vast majority of cases rely on the processing of personal data (i.e. on the collection, registration, storage, disclosure and destruction of data related to an identified or identifiable person), meaning that data protection rules are applicable.

Application of these rules will have different consequences on the set-up and management of whistleblowing schemes. The whole range of these consequences is detailed below in this document (see Section IV).

The Working Party notes that while existing regulations and guidelines on whistleblowing are designed to provide specific protection to the person making use of the whistleblowing scheme ("the whistleblower"), they never make any particular mention of the protection of the accused person, particularly with regard to the processing of his/her personal data. Yet, even if accused, an individual is entitled to the rights he/she is granted under Directive 95/46/EC and the corresponding provisions of national law.

---

[7] The U.S. Court of Appeals (1st Circuit) held on 5 January 2006 that SOX provisions on the protection of whistleblowers do not apply to foreign citizens working outside the US for foreign subsidiaries of companies required to comply with the remaining provisions of SOX.

Applying EU data protection rules to whistleblowing schemes means giving specific consideration to the issue of the protection of the person who may have been incriminated in an alert. In this respect, the Working Party stresses that whistleblowing schemes entail a very serious risk of stigmatisation and victimisation of that person within the organisation to which he/she belongs. The person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated.

The Working Party is of the view that proper application of data protection rules to whistleblowing schemes will contribute to alleviate the above-mentioned risks. It also takes the view that, far from preventing these schemes from functioning in accordance with their intended purpose, application of these rules will generally contribute to the proper functioning of whistleblowing schemes.

IV. ASSESSMENT OF THE COMPATIBILITY OF WHISTLEBLOWING SCHEMES WITH DATA PROTECTION RULES

The application of data protection rules to whistleblowing schemes implies deal with the question of the legitimacy of whistleblowing systems (1); application of the principles of data quality and proportionality (2); the provision of clear and complete information about the scheme (3); the rights of the person incriminated (4); the security of processing operations (5); the management of internal whistleblowing schemes (6); issues related to international data transfers (7); notification and prior checking requirements (8).

1. Legitimacy of whistleblowing systems (Article 7 of Directive 95/46/EC)

For a whistleblowing scheme to be lawful, the processing of personal data needs to be legitimate and satisfy one of the grounds set out in Article 7 of the data protection Directive.

As things stand, two grounds appear to be relevant in this context: either the establishment of a whistleblowing system is necessary for compliance with a legal obligation (Article 7(c)) or for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)).[8]

i) Establishment of a whistleblowing system necessary for compliance with a legal obligation to which the controller is subject (Article 7(c))

The establishment of a reporting system should have the purpose of meeting a legal obligation imposed by Community or Member State law, and more specifically a legal obligation designed to establish internal control procedures in well-defined areas.

At the present time, such an obligation exists in most EU Member States in the banking sector, for instance, where governments have decided to strengthen internal control, in particular with regard to the activities of credit and investment companies.

---

[8] Companies should be aware that in some Member States the processing of data on suspected criminal offences is subject to further specific conditions relating to the legitimacy of their processing (see *infra*, section IV, 8).

Such a legal obligation to put in place reinforced control mechanisms also exists in the context of combating bribery, in particular as a result of the implementation in national law of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Convention of 17 December 1997).

By contrast, an obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC. As a result, SOX whistleblowing provisions may not be considered as a legitimate basis for processing on the basis of Article 7(c).

However, in certain EU countries whistleblowing schemes may have to be put in place by way of legally binding obligations of national law in the same fields as those covered by SOX.[9] In other EU countries where such legally binding obligations do not exist, the same result may, however, be achieved on the basis of Article 7(f).

ii) Establishment of a whistleblowing system necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f))

The establishment of reporting systems may be found necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)). Such a reason would only be acceptable on condition that such legitimate interests are not "overridden by the interests for fundamental rights and freedoms of the data subject".

Major international organisations, including the EU[10] and the OECD,[11] have recognised the importance of relying on good corporate governance principles to ensure the adequate functioning of organisations. The principles or guidelines developed in these forums consist in enhancing transparency, developing sound financial and accounting practices, and thus improving the protection of stakeholders and the financial stability of markets. They specifically recognise an organisation's interest in putting in place appropriate procedures enabling employees to report irregularities and questionable accounting or auditing practices to the board or the audit committee. These reporting procedures must ensure that arrangements are in place for the proportionate and independent investigation of facts reported, which includes an adequate procedure of selection of the persons involved in the management of the scheme, and for appropriate follow-up action.

---

9 Dutch Corporate Governance Code, 9.12.2003, Section II, 1.6
Spanish Draft of Unified Code on corporate governance of listed companies, Chapter IV, 67(1)d). This Code has still to be examined by the Spanish Data Protection Authority in order to consider data protection implications.

10 European Community: Commission Recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board (OJ L 52, 25.2.2005, p. 51).

11 OECD: OECD Principles of Corporate Governance. 2004. Part One, Section IV.

Moreover, these guidelines and regulations stress that the protection of whistleblowers should be ensured and there should be appropriate guarantees protecting whistleblowers against retaliatory measures (discriminatory or disciplinary actions).[12]

Indeed, the goal of ensuring financial security in international financial markets and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing mattets and reporting as well as the fight against bribery, banking and financial crime or, insider trading appears to be a legitimate interest of the employer that justifies the processing of personal data by means of whistleblowing systems in these areas. Ensuring that reports on suspected accounting manipulations or defective account auditing, which may have an impact on the financial statements of the company and concern the legitimate interests of stakeholders in the financial stability of the company, actually reach the Board of directors with a view to appropriate follow-up is a critical concern for a public company, especially those listed in financial markets.

In this context, the US Sarbanes-Oxley Act may be considered as one of these initiatives adopted to ensure the stability of financial markets and the protection of legitimate interests of stakeholders by laying down rules that guarantee appropriate corporate governance of companies.

For all these reasons, the Working Party considers that in those EU countries where there is no specific legal requirement imposing the implementation of whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, and combating against bribery, banking and financial crime, data controllers still hold a legitimate interest in implementing such internal schemes in those fields.

However, Article 7(f) requires a balance to be struck between the legitimate interest pursued by the processing of personal data and the fundamental rights of data subjects. This balance of interest test should take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be put in place. In particular, Article 14 of Directive 95/46/EC provides that, when data processing is based on Article 7(f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them. These points are developed below.

2. Application of the principles of data quality and proportionality (Article 6 of the Data Protection Directive)

In accordance with Directive 95/46/EC, personal data must be processed fairly and lawfully;[13] they must be collected for specified, explicit and legitimate purposes[14] and not be used for incompatible purposes. Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[15] Combined, these latter rules are sometimes referred to as the

---

[12] See, for instance, UK Public Interest Disclosure Act 1998.

[13] Article 6(1)(a) Directive 95/46/CE

[14] Article 6(1)(b) Directive 95/46/CE

[15] Article 6(1)(c) Directive 95/46/CE

"proportionality principle". Finally, appropriate measures have to be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[16] The application of these essential data protection rules has a number of consequences as to the way in which reports may be made by an organisation's employees and processed by that organisation. These consequences are studied below.

i) Possible limit on the number of persons entitled to report alleged improprieties or misconduct through whistleblowing schemes

In application of the proportionality principle, the Working Party recommends that the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme, in particular in the light of the seriousness of the alleged offences to be reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

ii) Possible limit on the number of persons who may be incriminated through a whistleblowing scheme

In application of the proportionality principle, the Working Party recommends that the company putting in place a whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

iii) Promotion of identified and confidential reports as against anonymous reports

The question of whether whistleblowing schemes should make it possible to make a report anonymously rather than openly (i.e. in an identified manner, and in any case under conditions of confidentiality) deserves specific attention.

Anonymity might not be a good solution, for the whistleblower or for the organisation, for a number of reasons:

- being anonymous does not stop others from successfully guessing who raised the concern;
- it is harder to investigate the concern if people cannot ask follow-up questions;

---

[16] Article 6(1)(d) Directive 95/46/CE

- it is easier to organise the protection of the whistleblower against retaliation, especially if such protection is granted by law,[17] if the concerns are raised openly;
- anonymous reports can lead people to focus on the whistleblower, maybe suspecting that he or she is raising the concern maliciously;
- an organisation runs the risk of developing a culture of receiving anonymous malevolent reports;
- the social climate within the organisation could deteriorate if employees are aware that anonymous reports concerning them may be filed through the scheme at any time.

As far as data protection rules are concerned, anonymous reports raise a specific problem with regard to the essential requirement that personal data should only be collected fairly. As a rule, the Working Party considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement.

However, the Working Party is aware that some whistleblowers may not always be in a position or have the psychological disposition to file identified reports. It is also aware of the fact that anonymous complaints are a reality within companies, even and especially in the absence of organised confidential whistleblowing systems, and that this reality cannot be ignored. The Working Party therefore considers that whistleblowing schemes may lead to anonymous reports being filed through the scheme and acted upon, but as an exception to the rule and under the following conditions.

The Working Party considers that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint. In particular, companies should not advertise the fact that anonymous reports may be made through the scheme. On the contrary, since whistleblowing schemes should ensure that the identity of the whistleblower is processed under conditions of confidentiality, an individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. For that reason a scheme should inform the whistleblower, at the time of establishing the first contact with the scheme, that his/her identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. It is also necessary to make whistleblowers aware that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of the enquiry conducted by the whistleblowing scheme.

The processing of anonymous reports must be subject to special caution. Such caution would, for instance, require examination by the first recipient of the report with regard to its admission and the appropriateness of its circulation within the framework of the scheme. It might also be worth considering whether anonymous reports should be investigated and processed with greater speed than confidential complaints because of the risk of misuse. Such special caution does not mean, however, that anonymous reports should not be investigated without due consideration for all the facts of the case, as if the report were made openly.

---

[17] E.g. under the UK Public Interest Disclosure Act

iv) Proportionality and accuracy of data collected and processed

In accordance with Article 6(1)(b) & (c) of the Data Protection Directive, personal data has to be collected for specified, explicit and legitimate purposes and must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.

Given that the purpose of the reporting system is to ensure proper corporate governance, the data collected and processed through a reporting scheme should be limited to facts related to this purpose. Companies setting up these systems should clearly define the type of information to be disclosed through the system, by limiting the type of information to accounting, internal accounting controls or auditing or banking and financial crime and anti-bribery. It is recognised that in some countries the law may expressly provide for whistleblowing schemes also to be applied to other categories of serious wrongdoing that may need to be disclosed in the public interest[18] but these are outside the scope of this opinion; they may not apply in other countries. The personal data processed within the scheme should be limited to the data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

When facts reported to a whistleblowing scheme do not relate to the areas of the scheme in question, they could be forwarded to proper officials of the company/organisation when the vital interests of the data subject or moral integrity of employees are at stake, or when, under national law there is a legal obligation to communicate the information to public bodies or authorities competent for the prosecution of crimes.

v) Compliance with strict data retention periods

Directive 95/46/EC lays down that personal data processed shall be kept for the period of time necessary for the purpose for which the data have been collected or for which they are further processed. This is essential to ensure compliance with the principle of proportionality of the processing of personal data.

Personal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report.

Such periods would be different when legal proceedings or disciplinary measures are initiated against the incriminated person or the whistleblower in cases of false or slanderous declaration. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Such retention periods will be determined by the law of each Member State.

Personal data relating to alerts found to be unsubstantiated by the entity in charge of processing the alert should be deleted without delay.

---

[18] For instance, UK Public Interest Disclosure Act 1998.

Furthermore, any national rules relating to archiving of data in the company remain applicable. These rules may in particular access to the data kept in such archives, and specify the purposes for which such access is possible, the categories of persons who may have access to those files, and all other relevant security regulations.

3. Provision of clear and complete information about the scheme (Article 10 of the Data Protection Directive)

The requirement of clear and complete information on the system obliges the controller to inform data subjects about the existence, purpose and functioning of the scheme, the recipients of the reports and the right of access, rectification and erasure for reported persons.

Data controllers should also provide information on the fact that the identity of the whistleblower shall be kept confidential throughout the whole process and that abuse of the system may result in action against the perpetrator of the abuse. On the other hand, users of the system may also be informed that they will not face any sanctions if they use the system in good faith.

4. Rights of the incriminated person

The legal framework set by Directive 95/46/EC specifically emphasises the protection of the data subject's personal data. Accordingly, from a data protection point of view, whistleblowing schemes should focus on the data subject's rights, without damage to the whistleblower's ones. A balance of interests should be established between the rights of the parties concerned, including the company's legitimate investigation needs.

i) Information rights

Article 11 of Directive 95/46/EC requires individuals to be informed when personal data are collected from a third party and not from them directly.

The person accused in a whistleblower's report shall be informed by the person in charge of the scheme as soon as practicably possible after the data concerning them are recorded. Under Article 14, they also have the right to object to the processing of their data if the legitimacy of the processing is based on Article 7(f). This right of objection, however, may be exercised only on compelling legitimate grounds relating to the person's particular situation.

In particular, the reported employee must be informed about: [1] the entity responsible for the whistleblowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification.

However, where there is substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception to the rule provided by Article 11 is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case-by-case basis, and it should take account of the wider interests at stake.

The whistleblowing scheme should take the necessary steps to ensure that the information disclosed will not be destroyed.

ii) Rights of access, rectification and erasure

Article 12 of Directive 95/46/EC gives the data subject the possibility to have access to data registered on him/her in order to check its accuracy and rectify it if it is inaccurate, incomplete or outdated (right of access and rectification). As a consequence, the setting-up of a reporting system needs to ensure compliance with individuals' right to access and rectify incorrect, incomplete or outdated data.

However, the exercise of these rights may be restricted in order to ensure the protection of the rights and freedoms of others involved in the scheme. This restriction should be applied on a case-by-case basis.

Under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed.

In addition, data subjects have the right to rectify or erase their data where the processing of such data does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data (Article 12(b)).

5. Security of processing operations (Article 17 of Directive 95/46/EC)

i) Material security measures

In accordance with Article 17 of Directive 95/46/EC, the company or organisation responsible for a whistleblowing scheme shall take all reasonable technical and organisational precautions to preserve the security of the data when it is gathered, circulated or conserved. Its aim is to protect data from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access.

The reports may be collected by any data processing means, whether electronic or not. Such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for added data confidentiality.

These security measures must be proportionate to the purposes of investigating the issues raised, in accordance with the security regulations established in the different Member States.

Where the whistleblowing scheme is run by an external service provider, the data controller needs to have in place a contract for adequacy and, in particular, take all the appropriate measures to guarantee the security of the information processed throughout the whole process.

ii) Confidentiality of reports made through whistleblowing schemes

Confidentiality of reports is an essential requirement to meet the obligation provided for by Directive 95/46/EC to comply with the security of processing operations.

In order to meet the objective for which a whistleblowing scheme has been established and encourage persons to make use of the scheme and report facts which may show misconduct or illegal activities by the company, it is essential that the person who reports be adequately protected, by guaranteeing the confidentiality of the report and preventing third parties from knowing his/her identity.

Companies establishing whistleblowing schemes should adopt the appropriate measures to guarantee that the whistleblowers' identity remains confidential and is not disclosed to the incriminated person during any investigation. However, if a report is found to be unsubstantiated and the whistleblower to have maliciously made a false declaration, the accused person may want to pursue a case for libel or defamation, in which case the whistleblower's identity may have to be disclosed to the incriminated person if national law allows. National laws and principles on whistleblowing in the field of corporate governance also provide for the whistleblower to be protected from retaliatory measures for making use of the scheme, such as disciplinary or discriminatory action being taken by the company or the organisation.

The confidentiality of personal data must be guaranteed when it is collected, disclosed or stored.

6. Management of whistleblowing schemes

Whistleblowing schemes require careful consideration of how the reports are to be collected and handled. While favouring internal handling of the system, the Working Party acknowledges that companies may decide to use external service providers to which they outsource part of the scheme, mainly for the collection of the reports. These external providers must be bound by a strict obligation of confidentiality and commit themselves to complying with data protection principles. Whatever the system established by a company, the company must comply in particular with Articles 16 and 17 of the Directive.

i) Specific internal organisation for the management of whistleblowing schemes

A specific organisational must be set up within the company or the group dedicated to handling whistleblowers' reports and leading the investigation.

This organisation must be composed of specially trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations.

This whistleblowing system should be strictly separated from other departments of the company, such as the human resources department.

It shall ensure that, insofar as is necessary, the information collected and processed shall be exclusively transmitted to those persons who are specifically responsible, within the company or the group to which the company belongs, for the investigation or for taking the required measures to follow up the facts reported. Persons receiving this information shall ensure that the information received is handled confidentially and subject to security measures.

ii) Possibility of using external service providers

Where companies or groups of companies turn to external service providers to outsource part of the management of the whistleblowing scheme, they still remain responsible for the resulting processing operations, as those providers merely act as processors within the meaning of Directive 95/46/EC.

External providers may be companies running call centres or specialised companies or law firms specialising in collecting reports and sometimes even conducting part of the necessary investigations.

These external providers will also have to comply with the principles of Directive 95/46/EC. They shall ensure, by means of a contract with the company on behalf of which the scheme is run, that they collect and process the information in accordance with the principles of Directive 95/46/EC; and that they process the information only for the specific purposes for which it was collected. In particular, they shall abide by strict confidentiality obligations and communicate the information processed only to specified persons in the company or the organisation responsible for the investigation or for taking the required measures to follow up the facts reported. They will also comply with the retention periods by which the data controller is bound. The company which uses these mechanisms, in its capacity as data controller, shall be required to periodically verify compliance by external providers with the principles of the Directive

iii) Principle of investigation in the EU for EU companies and exceptions

The nature and structure of multinational groups means the facts and outcome of any reports may need to be shared throughout the wider group, including outside the EU.

Taking the proportionality principle into account, the nature and seriousness of the alleged offence should in principle determine at what level, and thus in what country, assessment of the report should take place. As a rule, the Working Party believes that groups should deal with reports locally, i.e. in one EU country, rather than automatically share all the information with other companies in the group.

The Working Party acknowledges some exceptions to this rule, however.

The data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature or the seriousness of the reported misconduct, or results from how the group is set up. Such communication will be considered as necessary to the requirements of the investigation, for example if the report incriminates a partner of another legal entity within the group, a high level member or a management official of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient legal entity, which provides equivalent guarantees as regards the management of whistleblowing reports as the organisation in charge of handling such reports in the EU company.

7. Transfers to third countries

Articles 25 and 26 of Directive 95/46/EC apply where personal data are transferred to a third country. Application of the provisions of Articles 25 and 26 will be relevant, namely, when the company has outsourced part of the management of the whistleblowing scheme to a third party provider established outside of the EU or when the data collected in reports are circulated inside the group, thus reaching some companies outside of the EU.

These transfers are particularly likely to occur for EU affiliates of third country companies.

Where the third country to which the data will be sent does not ensure an adequate level of protection, as required pursuant to Article 25 of Directive 95/46/EC, data may be transferred on the following grounds:

[1] where the recipient of personal data is an entity established in the US that has subscribed to the Safe Harbor Scheme;

[2] where the recipient has entered into a transfer contract with the EU company transferring the data by which the latter adduces adequate safeguards, for example based on the standard contract clauses issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2004;

[3] where the recipient has a set of binding corporate rules in place which have been duly approved by the competent data protection authorities.

8. Compliance with notification requirements

In application of Articles 18 to 20 of the Data Protection Directive, companies which set up whistleblowing schemes have to comply with the requirements of notification to, or prior checking by, the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority in as much as those operations are likely to present a specific risk to the rights and freedoms of the data subjects. This could be the case where national law allows the processing of data relating to suspected criminal offences by private legal entities under specific conditions, including prior checking by the competent national supervisory authority. This could also be the case where the national authority considers that the processing operations may exclude reported individuals from a right, benefit or contract. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.

V – CONCLUSIONS

The Working Party acknowledges that whistleblowing schemes may be a useful mechanism to help a company or an organisation to monitor its compliance with rules and provisions relating to its corporate governance, in particular accounting, internal accounting controls, auditing matters, and provisions relating to the fight against bribery, banking and financial crime and criminal law. They may help a company to duly implement corporate governance principles and to detect facts that would impact on the position of the company.

The Working Party emphasises that the establishment of whistleblowing schemes in the areas of accounting, internal accounting controls, auditing matters, and fight against bribery, banking and financial crime, to which the present opinion relates, must be made in compliance with the principles of protection of personal data, as enshrined in Directive 95/46/EC. It considers that compliance with these principles helps companies and whistleblowing schemes to ensure the proper functioning of such schemes. Indeed, it is essential that in the implementation of a whistleblowing scheme the fundamental right to the protection of personal data, in respect of both the whistleblower and the accused person, be ensured throughout the whole process of whistleblowing.

The WP stresses the principles of data protection, as laid down in Directive 95/46/EC, must be applied in full to whistleblowing schemes, in particular with regard to the rights of the accused person to information, access, rectification and erasure of data. However, given the different interests at stake, the WP recognises that application of these rights may be the object of restriction in very specific cases, in order to strike a balance between the right to privacy and the interests pursued by the scheme. However, any such restrictions should be applied in a restrictive manner to the extent that they are necessary to meet the objectives of the scheme.

Done at Brussels, 1 February 2006

For the Working Party

The Chairman
Peter Schaar

Délibération n°2006-281 du 14 décembre 2006 sanctionnant la société Tyco Healthcare France

14 Décembre 2006 - Thème(s) : Travail

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents M. Guy ROSIER, vice-président délégué, M. François GIQUEL, vice-président, M. Hubert BOUCHET, membre, Mlle Anne DEBET, membre et M. Bernard PEYRAT, membre ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n°2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2006-144 adoptée par la CNIL le 10 mai 2006 ; Vu la décision de mission de contrôle n° 2006-074C ; Vu le rapport de M. Emmanuel de GIVRY, commissaire, notifié à la société Tyco Healthcare France le 27 octobre 2006 et les observations en réponse reçues le 24 novembre 2006.

Après avoir entendu, lors de la réunion du 14 décembre 2006, M. Emmanuel de GIVRY, commissaire, en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations. Après avoir entendu, lors de la réunion du 14 décembre 2006, les observations orales de Maître LORELEI, avocat, représentant la société Tyco Healthcare France, celle-ci ayant pris la parole en dernier.

Constate les faits suivants :

1. La société Tyco Healthcare France a déclaré à la CNIL le 22 septembre 2004 un traitement de données ayant pour finalité la « gestion des carrières à l'international ». Par courrier en date du 21 février 2005, la CNIL lui a demandé de lui faire parvenir certains éléments d'information indispensables à l'instruction de ce dossier. La société Tyco Healthcare France n'a apporté aucune suite satisfaisante aux demandes de la Commission réitérées dans ses courriers des 19 septembre 2005 et 21 mars 2006. En effet, la réponse adressée par la société Tyco Healthcare France SAS le 4 avril 2006 n'a pas permis d'apporter les réponses à l'ensemble des questions formulées par les services de la CNIL dans le cadre de l'instruction du dossier de déclaration (le descriptif précis des finalités exactes recherchées, les cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données).

2. Au regard des faits précités, la Commission a, par délibération adoptée le 10 mai 2006, mis en demeure la société Tyco, sous dix jours, de répondre aux questions posées par la CNIL dans ses courriers (courriers des 21 février, 19 septembre 2005, 21 mars 2006) ou de lui indiquer que le traitement précité avait été abandonné.

3. En réponse à la mise en demeure, la société Tyco Healthcare France a indiqué, par courrier du 1er juin 2006, que : « *Le groupe Tyco au niveau international devait scinder les 4 secteurs d'activités qui le constituent actuellement en entités indépendantes. Cette scission doit intervenir d'ici la fin de l'année calendaire. Par conséquent les procédures et les demandes d'information qui avaient été mises en place sont dans les circonstances actuelles suspendues* ».

4. La CNIL ne s'estimant pas suffisamment informée par cette réponse sur le sort exact ayant été finalement réservé au traitement objet de la mise en demeure a fait procéder à une mission de contrôle sur place le 12 juillet 2006 dans les locaux de la société Tyco Healthcare France. A cette occasion, les services de la CNIL ont constatée que le traitement objet de la mise en demeure, contrairement à ce qui avait été affirmé, était bien utilisé par la société Tyco Healthcare France. Au regard des documents communiqués (« *International Database Project Update, Data Auditing and Next Steps, June 2006* » et « *Guide de l'administrateur, Administration et traitement des données pour la base de données internationales* »), le traitement précité apparaît comme un outil de gestion essentiel, au plan mondial, de la politique salariale du groupe Tyco dont les finalités dépassent largement la finalité de « reporting » visée dans la déclaration du 22 septembre 2004. Lors de la mission de contrôle sur place, il a également été constaté que de strictes et récentes procédures étaient mises en œuvre pour que la société Tyco Healthcare France alimente de façon régulière la base de données avec les informations concernant les salariés français.

5. Il ressort de ce qui précède que les faits constatés sur place le 12 juillet 2006 étaient en contradiction avec la réponse adressée par la société Tyco Healthcare France le 1er juin 2006 puisque celle-ci n'a ni « suspendu » la mise en œuvre du traitement objet de la mise en demeure ni répondu à l'ensemble des questions posées concernant les modalités exactes de fonctionnement du traitement précité. En effet, s'agissant tout d'abord du descriptif précis des finalités recherchées et des fonctionnalités de l'application, dans son courrier du 4 avril 2006 la société Tyco Healthcare France indique que « *la finalité de cette base de données est purement celle d'un « reporting » vis à vis de notre hiérarchie européenne en*

ressources humaines ». Un document interne datant de juin 2006 communiqué aux services de la CNIL lors de la mission de contrôle du 12 juillet 2006 indique pourtant (« *International Database Project Update, Data Auditing and Next Steps, June 2006* »), concernant le traitement précité, que celui-ci sert à la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle, etc. Lors de la réunion du 14 décembre 2006, l'avocat représentant la société Tyco Healthcare France a également indiqué oralement que le traitement objet de la mise en œuvre avait également pour finalité de gérer la « mobilité interne ».

Dès lors, la Commission ne s'estime toujours pas informée sur le descriptif précis des finalités recherchées par le traitement déclaré le 22 septembre 2004 par la société Tyco Healthcare France comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006. S'agissant ensuite des cas précis dans lesquels des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis, le courrier du 4 avril 2006 se limite à indiquer que « *ces données peuvent être transmises du Royaume-Uni aux Etats-Unis si notre hiérarchie juge opportun de le faire* ». Si le contrôle du 12 juillet 2006 a permis d'établir une communication d'informations concernant le traitement objet de la mise en demeure entre la société Tyco Healthcare France et les locaux du groupe Tyco en Angleterre et aux Etats-Unis, il n'a pas été possible d'obtenir des informations précises sur les motifs liés à cet envoi d'informations. Dès lors, la Commission ne s'estime toujours pas correctement informée des cas précis où des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

S'agissant encore des lieux exacts d'implantation des serveurs et des systèmes, seul un schéma technique a été communiqué aux services de la Commission (« *Schéma de fonctionnement informatique Tyco Healthcare France* ») mais les adresses exactes des centres informatiques n'ont pas été communiquées à ce jour.

S'agissant des questions posées concernant les destinataires exacts des données et la durée de conservation des données, la Commission ne dispose à ce jour d'aucune réponse précise.

S'agissant enfin des mesures de sécurité assurant la confidentialité des données, si la mission de contrôle du 12 juillet 2006 a permis d'établir que l'accès aux ordinateurs de la société Tyco Healthcare France est sécurisé par mot de passe, la Commission ne dispose à ce jour d'aucune information technique précise sur les conditions de sécurité liées à la conservation des données en Angleterre et aux Etats-Unis.

Dès lors, la Commission ne s'estime toujours pas correctement informée sur les lieux exacts d'implantation des serveurs et des systèmes, les destinataires exacts des données, la durée de conservation des données et les mesures de sécurité assurant la confidentialité des données comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

6. Dans ses observations en réponse du 24 novembre 2006 et lors de la réunion du 14 décembre 2006, la société Tyco Healthcare France soutient que la proposition de sanction proposée par le rapporteur serait mal fondée sur le plan juridique dans la mesure où celle-ci ne s'appuierait sur aucune mise en demeure préalable mais uniquement sur la réalisation de la mission de contrôle du 12 juillet 2006. Sur ce point, la Commission observe qu'une procédure de sanction peut être engagée lorsque le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée (article 45 de la loi du 6 janvier 1978 modifiée le 6 août 2004).

La présente procédure de sanction s'appuie ainsi sur la mise en demeure prononcée par la CNIL le 10 mai 2006 et sur la réponse adressée par la société Tyco le 1er juin 2006. Il convient par ailleurs de rappeler que dans le cadre de l'analyse de la réponse adressée par la société Tyco le 1er juin 2006, la CNIL était en droit de procéder à une mission de vérification sur place afin, de vérifier la réalité des informations qui lui avaient été communiquées. La Commission estime à cet égard que les informations transmises par la société Tyco Healthcare France dans son courrier du 1er juin 2006 ne permettaient pas de connaître le sort exact ayant été réservé au traitement objet de la mise en demeure du 10 mai 2006. Au surplus, la société Tyco Healthcare France relève dans ses observations du 24 novembre 2006 que la décision de mission de contrôle n° 2006-074C ne visait pas formellement la mise en demeure du 10 mai 2006. Sur ce point, la Commission estime que l'existence d'une procédure de mise en demeure n'a, à cet égard, aucune incidence sur le formalisme à respecter pour la réalisation d'une telle mission de contrôle. La Commission considère par conséquent que la procédure de sanction est pleinement régulière.

7. La société Tyco a par ailleurs fait valoir dans ses observations du 24 novembre 2006 et lors de la réunion du 14 décembre 2006 que les informations communiquées lors de la mission de contrôle ne concerneraient pas le même traitement que celui visé dans la mise en demeure du 10 mai 2006. La Commission observe que les vérifications opérées sur place le 12 juillet 2006 par les services de la CNIL ont permis de constater que le traitement déclaré par la société Tyco Healthcare France le 22 septembre 2004 (« gestion des carrières à l'international »), comportait, comme indiqué précédemment, d'autres fonctionnalités relatives à la gestion des ressources humaines telles que par exemple la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle ainsi que la mobilité interne. Ces fonctionnalités, qui peuvent être rattachées à une finalité de gestion des carrières à l'international, n'étaient pas décrites dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004.

La Commission observe par ailleurs que les captures d'écran réalisées par les services de la CNIL lors du contrôle du 12 juillet 2006 sont concordantes s'agissant des catégories de données collectées et utilisées avec les « champs » informatiques figurant dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004 (données démographiques concernant les salariés, données sur la situation administrative des salariés, données concernant la localisation géographique des salariés, données sur la rémunération des salariés, etc.).

Dès lors, la Commission considère que les vérifications opérées par la CNIL le 12 juillet 2006 concernaient bien le traitement visé dans la mise en demeure du 10 mai 2006. 8. Il ressort de l'ensemble de ce qui précède que la société Tyco Healthcare France ne s'est pas conformée à la mise en demeure de la CNIL du 10 mai 2006 puisqu'elle n'a pas communiqué les éléments demandés par la CNIL concernant le traitement déclaré le 22 septembre 2004 (le descriptif précis des finalités exactes recherchées, le cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données) et qu'elle n'a pas cessé la mise en œuvre de celui-ci. La Commission observe à cet égard que la société Tyco Healthcare France n'a manifestement pas pris la mesure de la gravité des manquements qui lui sont reprochés concernant son manque de coopération et de transparence.

En conséquence, la Commission décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre de la société Tyco Healthcare France sise 2 rue Denis Diderot, La clef de Saint Pierre à Elancourt (78), compte tenu de la gravité des manquements commis, une sanction pécuniaire de 30.000 euros.

Par ailleurs, la Commission enjoint la société Tyco Healthcare France de répondre, sous dix jour à compter de la notification de la présente délibération, à l'ensemble des demandes formulées par la CNIL dans sa mise en demeure du 10 mai 2006.

La présente décision sera rendue publique.

Le président, Alex Türk

Dernière modification : 16/07/08