ROADMAP TO THE EC DRAFT DIRECTIVE'S NEW TEXT

This report is a roadmap to the EC Data Protection Draft Directive, adopted by the Commission on 15 October and published in the Official Journal (OJ C311) on 27 November. The text has been summarized and simplified drawing on the explanatory memorandum where necessary. They were published together as COM (92) 422 final.

CHAPTER 1
GENERAL PROVISIONS

Article 1 Objectives

Member States shall ensure both the protection of natural persons' rights with respect to the processing of their personal data, *in particular their right to privacy*, and the free flow of this data between Member States.

Article 2 Definitions

See box below.

Article 3 Scope

The Directive covers both *automated and manual processing* of personal data, with the exception of processing in respect of an activity outside Community law, or processing for a purely private and personal activity.

Article 4 National law applicable

Each Member State shall apply the Directive to all processing of personal data within its territory when the controller is established there or when, through an agent, he uses means situated in that territory.

ARTICLE 2 - DEFINITIONS

PERSONAL DATA - any information relating to an identified or identifiable natural person; 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.

PROCESSING OF PERSONAL DATA ("PROCESSING") - any operation or set of operations which is performed upon personal data, whether or not by automatic means.

PERSONAL DATA FILE ("FILE") - any structured set of personal data, whether centralized or geographically dispersed, which is accessible according to specific criteria and whose object or effect is to facilitate the use or comparison of data relating to the data subject or subjects.

CONTROLLER - any natural or legal person, public authority, agency or other body who processes personal data or causes it to be processed and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them.

PROCESSOR - any natural or legal person who processes personal data on behalf of the controller.

THIRD PARTY - any natural or legal person other than the data subject, the controller and any person authorised to process the data under the controller's direct authority or on his behalf.

THE DATA SUBJECT'S CONSENT - any express indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed, on condition he has available information about the purposes of the processing, the data or categories of data concerned, the recipient of the personal data, and the name and address of the controller and of his representative if any.

The data subject's consent must be freely given and specific, and may be withdrawn by the data subject at any time, but without retrospective effect.

CHAPTER 2
GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5 Lawful Processing

The processing of personal data is lawful only if carried out in accordance with Chapter 2. However, Member States may determine more precisely the circumstances in which the processing of personal data is lawful.

Section I Principles relating to data quality

Article 6

This article includes the *basic data protection principles* that are also in Article 5 of Council of Europe Convention 108 on Data Protection and national data protection laws in Europe.

The controller shall ensure that personal data is: processed fairly and lawfully; collected and used for specified, explicit and legitimate purposes; adequate, relevant and not excessive; accurate and up to date and, finally, is stored in a form which identifies data subjects for the intended purposes for a period no longer than necessary.

Section II Principles relating to the grounds for processing data

Article 7

This article specifies a number of *alternative conditions* for the lawful processing of personal data.

Personal data may be processed:

1. if the data subject has consented to it, or,
2. if he has not, only if processing is necessary for one of the following: the performance of a contract with the data subject or taking steps preliminary to entering into a contract; or
3. compliance with an obligation under national or Community law; or
4. the protection of the vital interests of the data subject; or
5. the performance of a task in the public interest or by a public authority; or
6. in pursuit of the general interest or the legitimate interests of the controller or a third party, unless the interests of the data subject prevail.

Section III Special categories of processing

Article 8

The processing of certain categories of *sensitive data* (for example, data revealing racial or ethnic origin) is prohibited, except:

1. where the data subject has given his written consent, or
2. the processing is conducted by prescribed non-profit making organisations (for example, a trade union) under specified conditions, or
3. where there is manifestly no infringement of privacy or fundamental freedoms.

Further, Member States may, on important public interest grounds, derogate under strict conditions from the general prohibition of processing sensitive data. In particular, data on criminal convictions may be held, but only by judicial and law-enforcement authorities and by those directly concerned with the convictions.

Ultimately, it is left to Member States to regulate the use of a national identification number.

Article 9 Processing of personal data and freedom of expression

The Directive imposes on Member States the obligation to prescribe exemptions from its provisions in relation to processing of personal data solely for *reporting purposes* by the press, the audio-visual media and journalists.

Section IV Information to be given to the data subject

Article 10 The existence of a data processing operation

On request, the data subject is entitled to know of the existence of a data processing operation, its purposes, the identity of the data controller, his name and address, the categories of data involved and any third party involved. Member States may, on the grounds of public policy (Art. 14(1)), lay down exceptions to this rule.

Article 11 Collection of data from the data subject

The controller must ensure that the data subject is informed of the following *minimum information:* the purpose(s) of the proposed processing; the obligatory or voluntary nature of the data subject's responses to the questions asked; the consequences of failing to respond; the identity of the recipient(s) of the data; the right of the data subject to access to, and rectification of, the data; and finally the identity and address of the controller or his representative.

Exceptions to this rule are limited to cases where informing the data subject would hinder or prevent the exercise of the public authority's functions or the maintenance of public order.

Article 12 Disclosure to a third party

There is an obligation on the controller to ensure that in cases of lawful processing of personal data without the data subject's consent (Art. 7 (b), (c), (e), or (f)), the latter is *informed of the disclosure to a third party at an appropriate time* and not later than the first disclosure.

The data subject must be informed at least of: the name and address of the controller or his representative, the purposes of the processing, the categories of data, the data recipients and the existence of rights of access, rectification and objection.

This rule does not apply in cases where: the data subject has already been informed about the possible disclosure; the disclosure is required by law; and the data is disclosed for reasons of public law or policy (Art. 14(1)).

The supervisory authority may be granted power to authorize, subject to safeguards, an exemption from the obligation to inform the data subject. This will be the case when the requirement of information to the data subject is impossible to fulfil or involves disproportionate effort, or is properly subordinate to the overriding legitimate interests of the controller or a third party.

Section V The data subject's rights of access to data

Article 13 Right of access

The data subjects' *rights of access* gives them, at reasonable intervals and without excessive delay or expense, confirmation of the existence of their personal data; a copy of the data in an intelligible form; an indication of the data's source and use; a right of refusal to exercise the right of access against their will; rectification of inaccurate or incomplete data or erasure or blocking (where appropriate) of data and notification of such action to any third party to whom the data has been disclosed; and finally, information as to the reasoning applied in any automated processing operations of which the result is invoked against them.

Article 14 Exceptions to the right of access

The exceptions are based on the grounds of *public policy* (national security, defence, criminal proceedings, public safety, an economic and financial interest, a monitoring or inspection function, an equivalent right of another person). In these cases, the supervisory authority is empowered, at the data subject's request, to verify the lawfulness of the processing.

Further, the right of access may, in respect of data collected for *statistical purposes,* be limited where the person concerned can no longer be identified.

Section VI The data subject's right to object

Article 15 Objection on legitimate grounds

The data subject *may object at any time* on legitimate grounds to the processing of personal data, after which the controller must cease the processing.

The controller must ensure that the data subject has been expressly given the opportunity to have his data erased free of charge before personal data is disclosed to third parties, or used for the purposes of marketing by mail.

Article 16 Automated individual decisions

Every natural person has the right not to be subjected to an administrative or private decision *adversely affecting him* where such decision is based solely on automated processing defining a personality profile.

Exceptionally, provided there are suitable measures to safeguard data subject's legitimate interests (including allowing him to defend his point of view), such a decision may be taken in the course of entering into or in the performance of a contract, or when it is authorised by superior legislation.

Section VII Security of processing

Article 17 Technical and Organizational Measures

The controller, processor or any person who shares responsibility for carrying out the processing, must take appropriate technical and organizational measures which shall *ensure a suitable level of security,* protection of personal data against accidental, or unlawful destruction or loss, unauthorized alteration, disclosure or any other form of unauthorised processing.

The appropriate level of security shall depend on the state of the art, the nature of the data to be protected, and an evaluation of the potential risks involved. Appropriate security shall also apply to the transmission of personal data within a network. The controller must ensure that remote access takes place within the limits of lawful processing. Anyone working with personal data shall not disclose it to third parties without the controller's agreement, unless required by national or Community law.

Section VIII Notification

Article 18 Obligation to notify the supervisory authority

There is an obligation on the controller to notify the supervisory authority before conducting the processing of *data of the same type intended to serve a single purpose* or several related purposes, including at least the following specified information:

1. the name and address of the controller or his representative
2. the purpose(s) of the processing
3. the type(s) of data subject
4. a description of the data processed
5. the types of third parties to whom the data is disclosed
6. proposed transfers of data to third countries outside the European Community
7. a description of data security measures (Art 17)

Any subsequent change in the above information must be notified to the supervisory authority.

In instances of processing which pose a *specific risk to the rights and freedoms of the individual,* the supervisory authority has the right to examine the notification and must give a decision within 15 days of being notified. In some cases, such instances may be authorised beforehand by law or supervisory authority decision.

Article 19 Simplification of and exemption from the obligation to notify

There is an obligation on Member States to provide specific measures to simplify or *exempt exclusively from the obligation to notify,* certain types of processing which do not adversely affect the rights and freedoms of data subjects.

The Directive gives the following examples of some of these categories of processing:

- the production of correspondence/papers;
- the satisfaction of legal, accounting, tax or social security duties;
- the consultation of documentation services accessible to the public.

Simplification or exemption measures shall be adopted either by or after consulting the supervisory authority and shall specify for each type of processing:

1. the purpose(s) of the processing
2. a description of the data
3. the type(s) of data subject
4. the third parties to whom the data will be disclosed
5. the data's storage time
6. where appropriate, the conditions under which the processing is to be carried out.

Simplication or exemption from notification do not release the controller from any other of the directive's obligations.

Article 20 Manual processing operations

Member states *may lay down conditions* under which the provisions on notification, simplification and exemption from the obligation to notify apply to manual processing.

Article 21 Register of notified processing operations

The register of notified processing operations, including all relevant information, *shall be maintained by the supervisory authority* and may be inspected by any person.

CHAPTER 3
JUDICIAL REMEDIES, LIABILITY AND PENALTIES

Article 22 Judicial remedies

It is for *Member States to provide* for the right of every natural person to a judicial remedy for any breach of the rights given by the Directive.

Article 23 Liability

Member States shall provide that any natural person should be *entitled to compensation* from a controller for damage suffered as a result of unlawful processing.

In the case of loss or destruction, or unauthorized access to data, the controller may be relieved from liability if he proves that he took suitable steps to comply with the data security requirements.

Article 24 Processing on behalf of the controller

When processing is carried out on his behalf, the controller must ensure that the necessary *security and organizational measures are taken* and must select a processor who provides sufficient guarantees in that respect.

The processor shall not exceed the powers stipulated in the written contract with the controller and, in particular, shall not, without the controller's agreement, disclose data to a third party. Further, he shall comply with national provisions adopted pursuant to the Directive.

Article 25 Penalties

It is left to the Member States to provide in their national law for penalties *against any person not complying* with the national provisions adopted pursuant to the Directive.

CHAPTER 4
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 26 Principles

The transfer of personal data to a third country is, in principle, allowed only if the third country concerned ensures an *adequate* level of protection which is to be assessed in the light of all the circumstances surrounding that particular data transfer operation.

MEASURING ADEQUACY OF DATA PROTECTION OUTSIDE THE EC

In assessing the adequacy of the level of protection afforded by a third country, particular account shall be taken of the:

1. nature of the data;
2. purpose(s) and duration of the proposed processing operation;
3. legislative provisions both general and sectoral in force in the third country in question; and
4. professional rules which are complied with there.

However, even in the absence of an adequate level of protection in the receiving country, the transfer of data may take place on condition that: the data subject has consented to the proposed transfer; the transfer is necessary, either preliminary to or for the performance of a contract between the data subject and the principal - and the data subject has been informed that the data may be transferred to a country outside the European Community which does not ensure an adequate level of protection; on important public policy grounds; or to protect vital interests of the data subject.

When the Commission finds, whether from Member States (who are obliged to inform the Commission) or from other sources, that the requirement of an adequate level of protection is not fulfilled, to the extent resulting in harm to the Community or a member state, it may enter into negotiations with the third country with a view to remedying the situation.

The Commission's decision that a third country provides an adequate level of protection may be based on the country's international commitments or its domestic law.

Article 27 Particular measures

A Member State may authorize a transfer of data to a third country not satisfying the requirements of an adequate level of protection, if the controller shows good reason for such a transfer, in particular, due to *contractual provisions which guarantee the exercise of the data subject's rights*. The member state shall inform the Commission and the other member states *in good time* of a proposed authorization.

Any Member State or the Commission can, after having been informed by a Member State of its proposal to grant such authorization, object to it before it takes effect. Then the Commission shall take appropriate measures after consulting the advisory committee.

CHAPTER 5
CODES OF CONDUCT

Article 28 National codes

It is left to the Member States to give effect to the codes of conduct drawn up by trade associations providing *additional regulation for the special features of particular sectors*. The supervisory authority must consult the views of data subjects before approving a code and its official publication. The codes may be subsequently extended or amended following the same procedure.

Article 29 Community codes

It is envisaged that, with the participation of trade associations, *Community codes of conduct will be drawn up* in order to properly apply the Directive to the particular circumstances of the given sector. They will be published, together with the opinion of the Working Party and the sector's representatives, in the EC Official Journal. The Working Party shall seek the views of data subjects.

CHAPTER 6
SUPERVISORY AUTHORITY AND WORKING PARTY

Article 30 Supervisory authority

An *independent public authority* shall be established at a national level by each Member State to supervise the protection of personal data and monitor the application of national provisions adopted to implement the Directive.

It shall be vested with strong investigative powers; effective powers of intervention, such as ordering the blocking or erasure of data; the power to bring an action before the courts for the infringement of the national implementing provisions. It will also hear complaints and must inform the complainant of the outcome.

Member States' supervisory authorities shall cooperate with one another, have a duty of confidence and make public an annual report.

Article 31 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

An independent *Working Party with advisory status* shall be established, composed of representatives of the national supervisory authorities and a representative from the Commission, who will also provide its secretariat, and an elected chairman.

Article 32 Tasks of the Working Party

It shall contribute to the *uniform application of national provisions,* informing the Commission if serious divergences between the laws and practices of Member States are found, give an opinion on the level of protection in the EC and in third countries and on Community codes of conduct, advise the Commission on any proposal for the addition of specific measures and make recommendations on all matters of data protection in the EC.

Its opinions and recommendations shall be transmitted to the Commission whose subsequent duty shall be to inform the Working Party of its action. The Working Party shall publish and make public an annual report and make it available to the Commission, the European Parliament and the Council.

CHAPTER 7
RULE-MAKING POWERS OF THE COMMISSION

Article 33 Exercise of rule-making powers

The Commission is empowered to *adopt the technical measures necessary* to apply the Directive to particular sectors or classes of processing and to ensure consistent application of the Directive, in accordance with the envisaged procedure involving the Advisory Committee.

Article 34 Advisory Committee

This Committee, composed of the Member States' representatives and chaired by the Commission representative, shall *assist the Commission* and deliver its opinion on draft measures proposed by the Commission. The latter shall take the highest account of this opinion and inform the Committee of its subsequent action.

Final provisions

Article 35 Timetable

Member States shall bring into force the measures implementing the Directive by 1 July 1994 and communicate to the Commission the texts of these national laws.

Member States shall *set a date,* no later than 30 June 1997, after which processing operations started before 1 July 1994 must comply with national implementing provisions.

Article 36 Implementation and Amendments

The Commission has an obligation to *report to the Council and the European Parliament* on the implementation of the Directive with, if necessary, any proposed amendments.

Article 37 Member States

The Directive is addressed to the Member States.

This report was written by Bojana Perovic, a Privacy Laws & Business correspondent.