

**E-call Driving Group,
Issues on Privacy.**

- 1. Introduction 2
- 2. DIRECTIVE 95/46/EC. 2
 - 2.1 Chapter I, general provisions, 3
 - 2.2 Chapter II, general rules on the lawfulness of the processing of personal data..... 5
 - 2.2.1 Section I, principles relating to data quality..... 5
 - 2.2.2. Section II, Criteria for making data processing legitimate. 5
 - 2.2.3. Section III, Special Categories of Processing. 6
 - 2.2.4. Section IV, Information to be given to the data subject..... 7
 - 2.2.5. Section V, the data subject’s right of acces to data..... 8
 - 2.2.6. Section VI, Exemptions and restrictions..... 8
 - 2.2.7. Section VII, the data subject’s right to object. 9
 - 2.2.8. Section VIII, confidentiality and security of processing..... 9
 - 2.2.9. Section IX, Notification. 10
 - 2.3 Chapter III, judicial remedies, liability and sanctions..... 11
 - 2.3 Chapter IV, Transfer of Personal data to third countries. 12
 - 2.4 Chapter V, Codes of Conduct. 12
 - 2.5 Chapter VI, supervisory authority and working party 12
 - 2.6 Chapter VII, Community implementing measures..... 13
- 3 National laws. 14
- 4 Best approach. 15

Author: Jan Malenstein.
Sr. Advisor ITS
KLPD.
Date : 8 April 2005.

1. Introduction.

Privacy still is considered to be a controversial issue, but is this really true? A number of years ago, each Member state had its own privacy regulations and laws. This meant that it was hardly impossible to exchange personal data across borders due to the many constraints and interpretations of Privacy. Even now, it is still a subject that turns up at almost any project or EU initiative and it is still debated in length.

This was recognised as a huge problem on which the Commission took action. The definite need to harmonise the privacy concept in the EU member states led to:

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.

This Directive had to become effective in September 1998 because it read in 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*", which was 24 October 1995. The Directive was published in the Official Journal of the European Union on 23 November 1995, No L 281/31.

But this was delayed till September 2002, due to the fact that quite a number of Member States were not able to transpose this Directive into national legislation, as was required by the Directive.

Finally, in September 2002, this EU Directive became effective in the whole of the European Union, all national laws on privacy either adjusted to be in line with the Directive or due to new lawgiving.

This instituted the basic principle that there can be no major differences in privacy legislation any more in the EU; there may be little add-ons in national legislation, but the EU Directive cannot be restricted by national lawgiving. This created a whole new situation, effectively a whole new ball game with a new set of rules.

Next to this a number of other EU legislation was initiated on specific privacy issues:

1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
2. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
3. Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

2. 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.

There are two key elements in this directive:

1. The protection of individuals with regard to the processing of personal data.
2. The free movement of such data.

Especially the 2nd element introduced a new key element that did hardly exist before. The exchange of personal data across the border of the EU, even across the internal borders was a very complex matter. Even in the area of crime fighting, the so-called Schengen Treaty, it was still a matter of authorisation of only a few officers that were authorised to perform this.

The free movement of personal data was introduced for a number of reasons:

- The establishment and functioning of the internal market requires that goods, persons, services and capital can flow freely across the borders, but also personal data related to that.
- The progress in information technology is making the processing and exchange of such data considerably easier.
- The economic and social integration resulting from the internal market development will lead to a substantial increase in cross-border flows of personal data between all involved in a private or public capacity in economic and social activities, but also between undertakings in different Member States.
- National authorities by virtue of Community law are obliged to collaborate and exchange personal data as to be able to perform their duties and to carry out tasks on behalf of an authority in another Member State.
- The increase in scientific and technical cooperatons and the coordinated introduction of new telecommunications networks in the EC necessitate and facilitate cross-border flows of personal data.

In the directive, it is implicitly stated that the right to privacy as laid down in Article 8 of the European Convention for the protection of Human Rights and Fundamental Freedoms, is fully recognised and maintained.

Moreover, of course, some exemptions are made as well:

- Activities regarding public safety, defence, State security or activities of the State in the area of Criminal laws fall outside the scope of Community law do not fall within the scope of this Directive.

2.1 Chapter I, general provisions,

Article 1 defines the scope 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 riht 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 Memer States for reasons connected with the protection afforded under paragraph 1.

Here's the unambiguous obligation to procect the right on privacy of **natural** people, note that this concerns natural people only.

But secondly, it is clearly stated that the free flow of personal data between Member States cannot be restricted nor prohibited for the sake of this protection. This is important because this means that there can be no reason to refuse the exchange of personal data, but one has to observe and comply to the rules as will be explained onwards in this paper.

Article 2 lists a number of definitions:

- a. **“Personal data”**. Any information relating to an identified or identifiable natural person (the data subject). Identifiable means once can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to this physical, physiological, mental, economic, cultural or social identity.
- b. **“Processing of personal data”**. 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”**. 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”**. 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”**. A natural or legal person, public authority, agency or any other body, which processes personal data on behalf of the controller.
- f. **“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 authorized to process the data;
- g. **“Recipient”**. 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. **“Data subject consent”**. 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.

This set of definitions clearly marks the spot. The data have to refer to a natural person, the processing and filing and the persons that are involved. Note the data subject consent, this is the part that has to be asked to everybody from whom, for whatever reason, personal data are requested and processed.

Article 3 defines the scope of and the exemptions from the Directive. Here it becomes clear that the processing has to be performed wholly or partly by automatic means but also otherwise if these personal data will form a part of a filing system or are intended to form part of a filing system.

The second paragraph of art. 3 excludes the following from the Directive:

1. Activities that fall outside the scope of Community law, as provided in Titles V and VI off the Treaty on the European Union. These titles concern provisions on a common foreign and security policy (Title V) and provisions on cooperation in the fields of justice and home affairs (Title VI). The latter Title had been shaped and defined in the Schengen Treaty on judicial cooperation between the Member States.
2. In any case to processing operations concerning public security, defence, State security (including the economic well-being of the Stae when the processing operations relates to State security matters) and the activities of the State in areas of criminal law (taken care off by Schengen).
3. The processing of personal data in the course of a purely personal or household activity.

This last one will reassure you all; your data in your PDA are not subjected to the Directive if this is for personal or household use only.

Article 4 defines the cases where national law, according to the Directive, is applicable and should hold provisions accordingly:

- 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. This applies for instance in embassies or aboard ships and planes.

- 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.

In the latter case (c), the controller has to appoint then a representative established in the territory of the Member State, without prejudic to legal actions that could be initiated against the controller himself.

This article holds important items for controllers that are operational in several Member States. As said in the introduction, there can be no major differences in privacy legislation any more in the EU; the EU Directive cannot be restricted by national lawgiving but there may be little additions in national legislation and those have to be taken into account fully for each Member State. The housework here is to list all these differing details and to comply with them.

2.2 Chapter II, general rules on the lawfulness of the processing of personal data.

Article 5 is the obligation for the Member States to determine more precisely the conditions under which the processing of personal data is lawful, but within the limits of the provisions in this chapter of the EU Directive.

The conditions are not specified in detail in the EU Directive but is left to the Member States to define. The principles of article 6 of the EU Directive have to be obeyed though.

Note that this leaves ample room for specific details to be filled in by the Member States as long as it remains in accordance with the EU Directive. This is however a complicating factor for international operating enterprises, see article 4 (c) hereabove.

2.2.1 Section I, principles relating to data quality.

Article 6 lists a number of principles concerning **data quality**.

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.

The controller is responsible that this is complied with.

2.2.2. Section II, Criteria for making data processing legitimate.

Article 7 lists a number of criteria for the **legitimacy** of personal data processing:

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).

2.2.3. Section III, Special Categories of Processing.

Article 8 defines **special categories** of processing.

This is an important article because here it is exactly listed what data are forbidden to be processed. These are the data that reveal or concern:

- Racial or ethnic origin.
- Political opinion.
- Religious or philosophical beliefs.
- Trade-union membership (still a very sensitive item in many countries!).
- Health or sex life.

And, of course, paragraph (2 - 3) of this article sums up the **exceptions**:

- a. If the data subject has given his or her explicit consent to process these data. This does not apply however if the laws of the applicable Member State provide that this prohibition may not be lifted by the data subject's consent.
- b. If 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-profitseeking 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.
- f. 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.

Paragraph (4) provides the possibility for the Member States, for reasons of substantial public interest, and subjected to the provision of suitable safeguards, to lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

This is not further defined in the EU Directive but is left to the discretion of the Member States.

Paragraph (5) is about the processing of data relating to **offences, criminal convictions or security measures**. These may be carried out only:

- a. Under the control of official authority,
- b. Or subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards under national law

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.

Paragraph 6 holds the obligation to notify the Commission on the derogations from paragraph 1 provided for in paragraphs 4 and 5.

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

Article 9 holds another important exemption: the processing of personal data solely carried out for journalistic purposes or for the purpose of artistic or literary expression, only if they are necessary to reconcile the right to privacy with the rules governing the freedom of expression.

2.2.4. Section IV, Information to be given to the data subject.

Article 10 is about the **information, to be given** to 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 deals with the provision of information in a situation where the data have **not been obtained from the data subject**.

Paragraph 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.

Paragraph 2 is again an exemption to paragraph 1. The obligation to provide information to the data subject is not applicable if 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. This applies particularly for statistical purposes or for the purposes of historical or scientific research.

2.2.5. Section V, the data subject's right of access to data.

Article 12 deals with the **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.

2.2.6. Section VI, Exemptions and restrictions.

Article 13 grants Member States the possibility to 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 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.

Paragraph 2 allows Member States to restrict the application of the right of access by means of a legislative measure 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. There is the obligation however to provide adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual.

2.2.7. Section VII, the data subject's right to object.

Article 14 institutes the right of the data object to **object**:

- a At least in the cases referred to in Article 7 (e) and (f) (**public interest, official authority invested in the controller or in a third party to whom the data are disclosed, necessary for legitimate interests**), 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 concerns automated individual decisions and the right of data subjects:

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:
 - o 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
 - o Is authorized by a law, which also lays down measures to safeguard the data subject's legitimate interests.

2.2.8. Section VIII, confidentiality and security of processing.

Article 16 says that 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.

This is an interesting article, it says that any operator only is allowed to process personal data according to his jobdescription or by the law. He cannot initiate any processing himself.

Article 17 concerns the **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:
 - a. - The processor shall act only on instructions from the controller,
 - b. - 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.

2.2.9. Section IX, Notification.

Article 18 is about the **obligation to notify** the supervisory authority.

This article contains a number of obligations:

1. The controller or his representative has to notify the supervisory authority (art 28) before the processing of personal data is carried out.
2. This may, again, be simplified or exempted in certain cases and following some conditions:
 - a. Where for categories of processing operations which are unlikely to affect adversely the rights and freedoms of data subjects, is specified:
 - i. Purposes of processing.
 - ii. Data or categories of data undergoing processing.
 - iii. Category or categories of data subject,
 - iv. Recipients or categories of recipients to whom data are to be disclosed.
 - v. Length of time that data are to be stored.
 - b. Where, in compliance with the national law, the controller appoints a personal data protection official, responsible for:
 - i. Ensuring in an independent manner the internal application of the national provisions.
 - ii. Keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), (**the register of processing operations**), 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) (**foundations etc. with a political, philosophical, religious or trade-union aim**).
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 is about the **Contents of notification**. It says that:

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;
 - a. A description of the category or categories of data subject and of the data or categories of data relating to them;
 - b. The recipients or categories of recipient to whom the data might be disclosed;
 - c. Proposed transfers of data to third countries;

- d. 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 is about **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 sets **rules for the publishing** 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 (**obligation to notify**) 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.

2.3 Chapter III, judicial remedies, liability and sanctions.

Article 22, 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, 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. 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, 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.

The height of the sanction is not specified in the EU Directive, that has been left to the Member states to define. For example, the Dutch privacy law institutes administrative sanctions and a maximum fine of 4500 euro.

2.3 Chapter IV, Transfer of Personal data to third countries.

Article 25 lays down the principles for the transfer of personal data to third countries.

1. The third country has to ensure an adequate level of protection.
2. This adequacy shall be assessed with particular consideration to:
 - a. The nature of the data
 - b. The purpose and duration of the proposed processing operation(s).
 - c. Country of origin and country of final destination.
 - d. Rules of the the law in the third country
 - e. Security measures to be complied to in the third country.
3. Member States and the Commission shall inform each other on cases where third countries do not ensure such an adequate level of protection.
4. If so, Member States shall take the measures to prevent any transfer of data.
5. The Commission shall at an appropriate time enter negotiations with such a country to remedy the situation.
6. The Commission may find that a third country has an adequate level of protection as a result from the procedure described in article 32 of the EU Directive.

Article 26 lists a numbe of **derogations**.

Again, a number of derogations from article 25 are listed:

1. Transfer of data to a 3rd country may take place if:
 - a. The data subject has given his unambiguous consent.
 - b. To perform and carry out according to a contract between the data subject and the controller.
 - c. The transfer is necessary or legally required based on grounds of public interest or legal claims.
 - d. The transfer is necessary in order to protect the vital interests of the data subject.
 - e. Transfer is made from a register, intended to provide information to the public and can be consulted by the public or by a person who can demonstrate a legal interest.
2. Authorised by a Member State if the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.
3. The Member State shall inform the Commission and other Member States of authorisations granted from paragraph 2.
4. If the Commission decides that proper safeguard is provided, the Member States shall take the necessary measures to comply with the Commission decision.

2.4 Chapter V, Codes of Conduct.

Only one article here, **article 27** lists a number of provisions for a code of Conduct, encouraged by Member States and the Commission. It is very generic. It is encouraged, not obliged, to draw up a code of conduct to contribute to the proper implementation of national provisions, pursuant from the EU Directive.

2.5 Chapter VI, supervisory authority and working party on the protection of individuals with regards to the processing of personal data.

Two items here are regarded: a supervisory authority and a working party.

Article 28 is about the supervision and lists the requirements for a 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:
 - a. **Investigative** powers, such as powers of access to data forming the subjectmatter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
 - b. 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 arning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions.
 - c. 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 institutes a so-called Working Party. This working party will operate on the EU level only. There is no need for a working party in each Member State. The Working party shall consist of representatives from the supervisory authorities of the Member States and Commission bodies and institutions. **Article 30 lists the duties** of the Working Party. Not explained in more detail here.

2.6 Chapter VII, Community implementing measures.

Here the usual institution of a Committee is described in Article 31, what its duties are and how it shall interact with the Commission. Not explained in more detail here.

Article 32 lists the final provisions:

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 is on the usual feedback to the EU parliament. Not explained in further detail here.

3 National laws.

In article 32 it is stated that the 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 Member States shall lay down the methods of making such reference.

The reference usually looks like this (Dutch example):

“Whereas it is necessary to implement Directive 95/46/EC of the European Parliament and of the Council of the European Union of 23 November 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of that data (OJ L 28 1); etc etc”

As said in the introduction, this Directive had to become effective in September 1998.

But this was delayed till September 2002, due to the fact that quite a number of Member States were not able to transpose this Directive into national legislation, as was required by the Directive.

Finally, in September 2002, this EU Directive became effective in the whole of the European Union, all national laws on privacy either adjusted to be in line with the Directive or due to new lawgiving.

In the Directive, a lot of issues are left to deal with by the Member States themselves, due to the subsidiarity principle:

- Purposes and means of processing are determined by national or Community laws or regulations (art. 2).
- The obligation for the Member States to determine more precisely the conditions under which the processing of personal data is lawful, but within the limits of the provisions in this chapter of the EU Directive (art. 5). This is a **key issue** as this is not defined exactly by the EU directive.
- Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use (art. 6 (e)).
- the possibility for the Member States, for reasons of substantial public interest, and subjected to the provision of suitable safeguards, to lay down exemptions in addition to those laid down in paragraph 2 (art 8) either by national law or by decision of the supervisory authority (art 8 par 4).
- 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 (art 8 par 5).
- Obligation to the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed (art 8 par 7).
- Granting Member States the possibility to adopt legislative measures to restrict the scope of the obligations and rights provided for etc etc (art 13 par 1).

- Allowing Member States to restrict the application of the right of access by means of a legislative measure 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 (art 13 par 2).
- Provision 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 (art 18 par 3).
- Provision 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) (*foundations etc. with a political, philosophical, religious or trade-union aim*) (art 18 par 4).
- Stipulation 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 (art 18 par 5).
- To 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 (art 20 par 1).
- The obligation to 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 (art 24).
- The provision, 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 (art 32 par 3).

Effectively, quite a number of issues are left to the Member States. For this reason, national lawgiving on privacy according to this EU Directive is much more substantial than the EU Directive itself which can be regarded as a Framework.

4 Best approach.

The details may differ from Member to Member States, but a basic, common approach can be applied.

Starting with the EU Directive, the general framework can be set up. Attention has to be paid to the question “who is the controller?” and the other definitions.

The framework has to address:

1. Principles relating to data quality.
2. Criteria for making data processing legitimate.
3. Special categories of processing.
4. Information to be given to the data subject.
5. The data subject’s right of access to data.
6. The data subject’s right to object.
7. Exemptions and restrictions.
8. Confidentiality and security of processing.
9. Notification.

Appointing official representatives and the personal data protection officer (art. 18 par 2 sub (b)) are first things to do. Take good notice of art 8, the “sensitive” data and stay away from that.

According to the provisions of the EU Directive, one has to describe the goal and purpose of the collecting and processing of personal data and all the related procedures.

A matrix of what exactly has to be covered would be helpful; also a matrix of the exemptions. It will be useful to use matrixes in which the EU Directive is positioned next to the national legislation to guarantee that nothing is missed.

The matrix identifiers can be according to the general principles, listed hereabove.

The controller has to identify who the public authority is. This is the authority to which one has to submit all the necessary details. In general, this authority may be consulted on beforehand as well to ensure that the correct procedure is followed. In the Dutch situation, this has proved to be very helpful. This authority can be consulted during operation as well. A good relationship with the public authority on privacy can be beneficial. This is an issue to be observed when a personal data protection officers is appointed.

The controller has to verify that all rights of the data subjects are respected and that provisions are documented on how to deal with those rights and how to inform the data subject.

Special attention needs to be paid to cross border exchange of personal data. When a controller is established in several member states, he has to comply with each law in each member state, which may lead to the definition of different procedures and obligations, depending on each member state individually. Next to that, the controller has to observe the rules to the transfer of personal data to third countries as well.

The last issue to observe is to monitor changes in legislation and to apply and include these as soon as possible in the processing of personal data.