EU-MIDT

Plenary

EU-MIDT/PLE/007-2006

Digital Tachograph System

Guidelines on Data protection

PREPARED BY: IDT Project
DATE: 24/04/2006
EU-MIDT Plenary – 007-2006

REF : EU-MIDT/PLE/007-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	IDT Project		27/08/2003
CHECKED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	24/04/2006
APPROVED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	24/04/2006
ISSUED BY	Secretariat	MIDT	17/05/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

IMPLEMENTATION OF THE DIGITAL TACHOGRAPH AND DATA PROTECTION

I. Preamble

The digital tachograph, as described in the Commission Regulation (EC) n° 1360/2002 will record and store digital data concerning individuals (drivers and enforcement officers) as well as legal persons (transport companies and approved workshops).

See requirements 73 to 105 b of the Commission Regulation (EC) n° 1360/2002 (pages 21 to 27).

These data will be accessible in different ways, depending on whether or not tachograph cards are used to get access to them, and in case tachograph cards are used, depending on the type of cards that will be used (driver, company, control or workshop cards) and of the mode of operation of the tachograph.

See requirements 007 to 11 of the Commission Regulation (EC) n° 1360/2002 (pages 13 to 14).

These data are also going to be **downloaded** and could also be **transferred** for freight and fleet management, but also for enforcement purposes.

See requirements 149 to 151 of the Commission Regulation (EC) n° 1360/2002 (page 31).

Finally, the digital tachograph will record and store data on tachograph cards, to be issued to the different persons submitted to the provisions of the Council Regulations (EEC) n° 3820/85 and 3821/85 as last amended.

See requirements 108 to 112 of the Commission Regulation (EC) n° 1360/2002 (pages 27 to 28).

Each tachograph card will then contain data, that will be accessible in different ways regulated notably and mainly by the Council Regulation (EC) n° 2135/98 as far as enforcement is concerned.

See requirements 194 to 212 b of the Commission Regulation (EC) n° 1360/2002 (pages 37 to 41) for the driver card.

See requirements 213 to 230 a of the Commission Regulation (EC) n° 1360/2002 (pages 41 to 42) for the workshop card.

See requirements 231 to 234 of the Commission Regulation (EC) n° 1360/2002 (pages 42 to 43) for the control card.

See requirements 235 to 238 of the Commission Regulation (EC) n° 1360/2002 (page 43) for the company card.

These data, their recording, their storing, the access to them, their transfer and their use fall under the scope of the Directive n° 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Therefore, Member States which have to implement the Regulation (EC) n° 2135/98 shall make sure that their implementation scheme does not contradict the data protection rules.

As the Directive n° 95/46/EC has been implemented in different ways by the Member States, this report will focus on :

- the way the Directive n° 95/46/EC has to be read ;
- the data enforcement officers and approved workshops are going to use ;
- the questions that will have to be answered by the Member States at the time they will implement the Regulation (EC) n° 2135/98 ;
- and the additional questions that the few Member States who have extended the protection of the individuals to legal persons will have to answer.

II. How to read the Directive n° 95/46/EC

1. Introduction

Information is an asset that we take for granted. It is also a tool, one that is of growing importance in today's society. There are real concerns about how information is used when it is about people. This is particularly the case when those "personal data" address matters that we consider to be very personal to us, matters such as our political and religions beliefs, our race, our health, and our sexuality. This kind of information can give the "data user" power over the "data subject", and experience has shown that this power can be abused. There is a consensus in our society that the use of personal data and related issues including the storage and security of such data, must therefore be controlled.

There is also a consensus that these concerns must be balanced by taking into account the legitimate need of the many commercial and non-commercial organisations to process personal data. To take some obvious examples:

- employers need to keep personal information about employees in order to pay wages, make social security contributions and fulfil their other legal and social obligations as employers.

- retailers need to be able to target advertising at the people who are likely to be interested in their products. Having access to personal information saves time and money and leads to more competitively priced products for consumers.

- hospitals and other health care providers must keep information about their patients including full medical records and any other factors that may have a bearing on patients' mental and physical well being. This is an essential requirement in delivering high quality health care.

- financial and credit organisations need personal data to minimise the risk of fraud and bad debts.

- small traders including local shops and newsagents need personal data for ordering, making deliveries as well as accountancy purposes.

- many professional people such as doctors, lawyers and accountants will often need personal data in order to give their clients the correct advice.

Balancing the different interests of data subjects and data users is not easy : if regulation is too little, then opportunities for abuse will arise and be taken advantage of by unscrupulous operators. If on the other hand, regulation goes too far, you end up by interfering unnecessarily with the legitimate business concerns of data users.

1.1 Getting the balance right

The Data Protection Directive ("the Directive"[1]) aims to provide a working balance between the needs of data subjects and those of data users by facilitating and encouraging the free movement of personal data while at the same time strictly protecting the privacy of the individual.

The Directive achieves this dual objective by laying down a framework for data protection law which will apply throughout the European Union.

In European terms, the Directive is an essential element in the establishment of a single European market where the principle of "free movement" requires that personal data should be able to move freely between the Member States and also, that the fundamental rights of individuals should be safeguarded. In the past, the different levels of protection afforded to individuals in Member States meant that this was not always the case.

With the Directive now in place and due to be implemented into the national law of the Member States by 24 October 1998, the regulatory obstacles to the free movement of personal data will be greatly reduced. It should be noted however that in keeping with the principle of "subsidiarity", the Directive leaves Member States a margin of choice in their implementation of some aspects of the Directive, allowing them to tailor their implementation to the existing situation in their Member State. This fact may lead to some disparities in the implementation of the Directive in some Member States which could have an effect on the movement of data within a Member State as well as within the European Union.

It will also have an impact on the way, in our case, the regulation (EC) n° 2135/98 will be implemented in the different Member States, as far as the data protection issues are concerned.

1.2 Advantages of a comprehensive data protection strategy

Some data users may anyway be tempted to see all data protection law, including the Directive, as a nuisance, acting as a restraint on their use of personal data and imposing unnecessary burdens. However, one could also say that this Directive can have some advantages including amongst others:

- harmonisation of data protection law throughout the EU. The implementation of the Directive will result in the harmonisation of Member State law greatly facilitating the free movement of data within the EU and putting an end to distortions of competition arising from the current differences in law between Member States. This means that Member States are no longer able to restrict or prohibit the freedom of movement of

[1] 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 the free movement of such data.

personal data by arguing, for example, that another Member State does not provide an adequate level of protection[2].

- promotion of good practices in managing data. The introduction of the Directive has encouraged all data users to review all stages of their management of personal data. In this regard, many of the provisions of the Directive merely advocate good practice. For example:

  - the fact that manual files are included is encouraging data users to get to grips with and rationalise their manual files and consider how these files should be dealt with in the future - should they, for example, be transferred to an electronic medium? Rationalising the information kept on manual files is as much to the benefit of the data user as that of the data subject;

  - the security provisions of the Directive should not be an issue as they merely reflect good practice and what many responsible data users have already being doing. It is in the interest of every data user to implement, maintain and monitor adequate levels of security.

- many of the obligations imposed on data users are subject to a large number of exceptions, alternatives and possible derogations. For example:

  - exceptions to the general prohibition against the processing of special categories of data (Article 8);

  - under Articles 10 and 11, the fact that the data subject need not be informed where (s)he already has the information or under Article 11, where providing the information involves "a disproportionate effort" (though these exceptions should be strictly interpreted);

  - possibility of exemption from or simplification of notification requirements where, inter alia, the processing is unlikely to adversely affect the rights and freedoms of data subjects (Article 18);

  - derogations to the general prohibition on transfers of personal data to third countries which do not ensure adequate levels of protection (Article 26).

- good customer relations. There is a growing concern among the general public relating to the amount of personal data that is stored on computer networks. Customers are entitled to expect that those handling information about them do so properly and

[2] Note however the point made in Section 1.1 that the Directive leaves Member States a margin of discretion in the implementation of some aspects of the Directive, and that this could lead to differences in the implementation of the Directive in some Member States.

responsibly. Customers will be reassured to know that the organisations with which they are doing business comply with data protection law including the data protection principles (Article 6). Many reputable data users already take great pains to let their customers know their data protection policy. They have round that this is an important element in building up their organisation's reputation with a view to establishing long term customer relationships. Data users that have not taken this approach to date may consider making a virtue of necessity.

- Member States. For Member States, the introduction of the Directive is an opportunity to review and possibly simplify existing laws on data protection and to bring national law in line with technological change.

- data subjects. Finally, we are all data subjects and as such, we all have an interest in ensuring that the information which is stored about us and the manner in which that information is used, is subject to strict controls. From the data subject's perspective, the Directive has introduced more transparency into the flows of personal data, including the right to be informed in circumstances covered by Article 11. Data users should take comfort from the fact that there is no indication that the introduction of the Directive will lead to a marked increase in subject access requests.

2. An Overview of the Directive

The purpose of the Directive is stated in Article 1 to be the protection of the fundamental rights and freedoms of individuals and to ensure the free flow of personal data between Member States. Member States are exhorted not to restrict the free flow of information for reasons to do with lack of harmonisation and therefore the application of the Directive in all Member States will create a common set of ground rules for the free movement of data throughout the European Union. External data havens might undermine this stated aim, and so the Directive contains rules on the export of data to third countries.

To the extent that the public sector is subject to EU law, then the same regime applies to the public sector as well as to the private sector.

This lack of distinction is a common theme in the Directive so, for instance, no distinction has been drawn between the format of data or the technology on which it is stored or transmitted.

Manual data are included if structured and accessible regardless of the fact that their storage may be geographically dispersed.

Processing is very widely defined so that all data are caught from collection to destruction.

A fundamental change for certain Member States is the concept that processing must now be based on a criterion of legitimacy as set out in Article 7 of the Directive. There is no longer an automatic right to process.

There are very few exceptions to the application of the Directive and such exceptions as there are limited to processing carried out by a natural person in the course of a purely personal or household activity. The only other two areas of exemption are those matters which fall outside the purview of the European Union and processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression but only to the extent that these exemptions are necessary to reconcile the right to privacy with the rules governing freedom of expression.

The mirror image of the requirement to process legitimately is the data subject's right to object to processing in some cases subject to conditions but in others, particularly for direct marketing, unconditionally.

The Directive contains very familiar statements on data quality which are derived from the traditional lists set out in the OECD guidelines and in the European Convention on Data Protection.

The Directive contains a prohibition on the processing of special categories of data relating to such issues as racial or ethnic origin, political opinions, religions or philosophical beliefs, trade union membership and the processing of data concerning health or sex life. However, this prohibition is subject to certain exceptions so long as the interests of the individual are protected.

The Directive draws a distinction between the circumstances where the data are and are not collected directly from the data subject. Article 10 and Article 11 respectively, contain prescribed lists of information which have to be given to the data subject in these two circumstances.

As might be expected, data subjects have rights of access to the data and a right to make their case known where an automated individual decision has been taken which is unfavourable to them.

The Directive provides for either notification or the publicising of processing operations where notification is not required. The Directive requires the establishment of a supervisory authority which has the power to carry out prior checking in respect of processing operations likely to present specific risks to the rights and freedoms of data subjects.

Member States are required to provide judicial remedies to support data subjects' rights with suitable sanctions and regimes of liability imposed on controllers and processors.

The Directive draws a distinction in respect of transfers to third countries between those third countries which have an adequate level of protection and those that do not.

Member States and the Commission are required to encourage the drawing up of codes of conduct for specific sectors.

Member States must establish public authorities to be the supervisory bodies for the administration of the Directive within the territory of each Member State but in addition a working party was established which includes a representative of the Commission. The working party is given responsibility to ensure harmonisation of application of the Directive and to give opinions on the level of protection in third countries.

The Directive prescribes the date by which Member States must implement it, and the period within which processing already under way when the implementing legislation comes into force must be brought into compliance. Each Member State must then apply its own national law to the processing of controllers established in its territory, or if not established in its territory, to processing elsewhere where its national law applies or where the processing uses equipment in its territory (other than merely for transmission of data).

3. Cost Effective Compliance

The purpose of this document is to promote cost effective compliance with the Directive, i.e., to encourage organisations to fully comply with the requirements of the Directive, but in ways that involve as little additional cost as possible.

The aim of this section of the document in particular is to highlight cost effective and practical means whereby Controllers and others involved in data processing can achieve compliance with the requirements of the Directive. Thus, the section reviews the Directive Article by Article, in each case setting out what the Article requires in operational terms, as well as suggesting cost effective solutions for compliance with these requirements.

The solutions that we highlight are "cost effective" insofar as they advocate a common sense approach to data protection that sees it as an integrated part of a good information management policy, something that carries significant direct benefits in terms of more efficient business administration, as well as indirect benefits such as better customer relations.

To make the section of more practical application, the section also includes examples of the types of notices and contractual clauses which are likely to be required by the Directive - it

goes without saying that these examples (which are voluntarily taken outside the scope of the implementation and use of the digital tachograph) are for illustrative purposes only and should not be relied on as satisfying the requirements of the Directive, and in particular the implementing laws in the Member States, many of which, at the time of writing, have not as yet been published.

Some general pointers towards cost effective compliance

It is useful to underline some general pointers towards cost effective compliance before entering into a more detailed discussion of the Directive, and the requirements that it introduces:

- **the deadline.** Controllers and others involved in data protection should keep in mind that most of the Directive had to be implemented in the Member States' domestic laws by 24 October 1998.

- **the data protection audit.** To see how the Directive and the regulation (EC) n° 2135/98 will impact their organisation, Controllers should consider "auditing" their management of information, and in particular, all their data processing operations, including those that are carried out by third parties, well before the 2004 deadline. To assist in this task, a model for a "data protection audit" which can be adapted to the needs of different types and sizes of organisation, is attached as Annex 2 to this document.

- **implementing change.** Following an audit some organisations may well conclude that they already comply with many of the requirements of the Directive and of the regulation (EC) n° 2135/98, either because these requirements reflect existing national law, or because the organisation itself unilaterally decided to meet these requirements in the past (it may have taken the view that they represent good practice - the security provisions of the Directive are a good example of this latter point).

  Where changes are necessary, Controllers should consider how they can be implemented cost effectively, i.e., in ways that entail minimal additional cost, and bring maximum benefits in terms for example, of improved information management and customer relations; this section of the document provides guidance in this respect. What should be underlined is that although almost all organisations will need to make some changes to comply with the Directive and with the regulation (EC) n° 2135/98, the cost of many of these changes can with foresight be minimised, for example, by being planned for in advance and integrated into on-going reviews and updates of the affected areas of an organisation's business (internal handbooks, contracts with

employees and third parties etc. are all matters that for many other reasons are subject to frequent revision).

There are aspects of the Directive and of the regulation (EC) n° 2135/98 that may require specialist professional advice which can of course be costly - for example, organisations may want specialist legal advice on the changes that may have to be made to data protection notices to bring them into line with Articles 10 and 11, as well as other changes that will have to be made in contracts with third parties, such as Processors.

Even in these cases there are cost effective solutions. For example, Controllers should take advantage of the advice and guidance which will be available externally and often free of charge from bodies such as the Supervisory Authority (see European Commission web site), the relevant department of government, local chambers of industry or commerce, or sectoral trade bodies. Where what is freely on offer is not sufficient, Controllers may consider joining forces with Controllers in other organisations that have similar concerns to share the cost of any professional advice that may be required.

The project leaded by the Swedish National Road Administration and granted by the European Commission could provide such facilities.

- **raising staff awareness.** It is not enough that the Controller is informed: it is important that all employees and other staff including external consultants with access to personal data understand their responsibilities with regard to the security and general management of that data.

3.1 Definitions - Article 2

3.1.1 Scope

Article 2 sets out the definitions of key terms used in the Directive.

3.1.2 Operational requirements

Though the definitions in themselves do not impose obligations on data users, they may result in broadening the scope of current data protection law in some Member States. In particular:

- "Processing of personal data". The definition of processing in the Directive, which is stated to be non-exhaustive, is broader than that in current legislation in some Member States;

- "Personal data filing system". Again, the effect of this definition may be to broaden the scope of data protection law in some Member States as it extends, with some limitations, to manual records;

- "Controller". The role of "Controller" is central to the system established by the Directive. The introduction of the role of Controller into organisations may involve the rethinking, and in some cases the restructuring, of existing roles and relationships between the various people involved in data protection; and

- "Processor". Because of the very wide definition of processing in the Directive, the concept of "Processor" will include those that collect data (including manual data) such as market research organisations which will find themselves, for the first time in some Member States, falling within the scope of data protection law.

Data users must pay particular attention to how the definitions are implemented into the national law of the different Member States. This implementation will most probably reflect arrangements under existing national law. In particular, data users should be aware of the responsibilities assigned to the different roles introduced by the Directive.

3.1.3 Compliance

The question of who is a controller may not always be obvious. Take the example of organisations where goods or services are sold through intermediaries, agents or independent contractors. Many financial services organisations sell their financial products through such third parties. Also the mail order industry is traditionally centred around local agents. In such industries it is often the third party intermediary or agent that collects the information from the customer and keeps a record of each customers details. The question arises as to whether the intermediary or agent is a Processor or a Controller. Very often the contract between the organisation and the intermediary or agent will set out who owns the very valuable customer information and what is to happen to it on termination of the contract. The parties will have to balance the benefits of ownership of valuable data against the costs of shouldering the burdens of complying with the Directive as a Controller, especially if the Controller is assuming this role for the first time because the Directive may have introduced a change of emphasis in the roles of the parties. However, the costs will often be viewed as slight when compared with the value which can be gained from exploiting the data.

It is recommended that organisations should review who is a Controller, a Processor, a third party or a recipient under the regulation (EC) n° 2135/98.

3.2. Scope of application - Article 3

3.2.1 Scope

Article 3.1 defines the scope of the Directive stating that it applies to " ... the processing of personal data, within the scope of Community Law, 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; a personal data filing system being any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."

At first glance, organisations are probably likely to find this statement of the scope of the Directive somewhat forbidding. However, note that Article 3.2 of the Directive makes two forms of processing of personal data not subject to its provisions:

- processing by an individual purely for a personal or household activity; and

- processing operations concerning national security and defence and the administration of criminal justice, and to other activities falling outside the scope of Community law.

3.2.2 Operational requirements

The scope of the Directive (subject to Article 3.2), extends to all automatic processing (which itself is a concept widely defined in Article 2), of information relating to an identifiable individual. It will also apply to personal data held on a manual file together with personal data only partly processed by automatic means, where such data are structured in a way that they are "accessible according to specific criteria".

3.2.3 Compliance

To comply with this provision, Controllers must:

- identify, and analyse the data processing performed by or on behalf of the organisation. This could include, for example, data on :

- clients;
- suppliers;
- employees.

Much of this data will not be personal (for example, company information), however there may be personal data included with it (for example, personal information regarding contacts within a client company). On the other hand, some of the data, such as parts of employee files, will clearly contain personal information;

- identify data held on manual files which can be seen as forming part of a "filing system";

- identify data which does not form part of a "filing system" and is not intended to form part of a filing system;

- with reference to Article 3.2, identify any activities involving the processing of personal data which fall outside the scope of Community law. The Directive will not apply to any such processing though national law may well apply to such processing;

- extend subject access systems to manual files falling within the Directive;

- consider necessary steps to comply with the provisions of Article 6 (Data Quality), Article 7 (Legitimacy of Processing), Article 8 (Special Categories of Data). Under the Directive, Member States are given the option of introducing these provisions into national law over a 12 year transitional period. Many Member States did not make use of this arrangement. It should be remembered that derogation from the application of these Articles only applies to manual files that are in existence on the date of implementation of the Directive into national law. All data collected and put in filing systems after that date should comply in full with the provisions of the Directive. Controllers who have manual data in existence at the date of implementation of the Directive into national law must provide data subjects with the right to obtain access, rectification, erasure or blocking of the data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the Controller immediately.

The main impact of this Article will be to bring the manual processing of personal data within the scope of the law in many Member States for the first time, though it should be underlined that not all manual processing will be subject to the Directive's requirements: the test would appear to be two fold, firstly is the filing system structured and secondly is the information contained within that structured filing system accessible according to specific criteria?

The inclusion of manual files under data protection law will have little impact on the many organisations which already run their business with fully automated filing systems and have limited manual files (typically, only on employees). However, at the other end of the scale are organisations which keep a large number of manual files in different departments, sometimes in different countries, with no centralised records of such files being kept.

The cost of compliance with the requirements of the Directive will vary greatly for these two extremes and only in the latter example should be an issue. It could be argued that in such cases, most of the changes necessitated by the Directive are probably long overdue and should lead to more efficient file management which, in the medium term, could result in significant savings in terms of time and money.

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- conduct a data protection audit particularly if this is the first occasion upon which data protection law will apply to an organisation's manual files. An example of a comprehensive questionnaire which could form the basis of a data protection audit is set out in Annex 1. Though such a comprehensive exercise will be necessary for larger and more complex organisations smaller organisations may consider carrying out a simple review of the data held in manual filing systems.

  This exercise is an essential first step to compliance with the Directive and should give the Controller an overall picture of data flows within the organisation.

- Manual files. All electronically held personal data comes within the Directive. Manual files will only be covered where they allow easy access to personal data. For this reason, Controllers should conduct a review of all manual files containing personal data and consider whether they are covered by the Directive. The opportunity should be taken to remove and destroy obsolete files and documents. Consideration should be given to future policy regarding manual files, for example: whether such files need to be maintained and if so, whether they should be transferred to another medium. Organisations could also consider the introduction of a gradual timetable for the transfer of manual files to an automated medium.

- Guidelines. Where manual files need to be retained, guidelines for employees should be drawn up on how to manage such files in the future. Such guidelines could, for example :

  - explain the status of manual files under data protection law;

- establish file "housekeeping" principles e.g., what information should be maintained on the files, and for how long;

- explain and introduce the "data quality principles" in accordance with Article 6, underlining that they must apply to all data collected and put in filing systems;

- explain and introduce security measures in line with Article 17;

- explain data subjects' rights of access under Article 12;

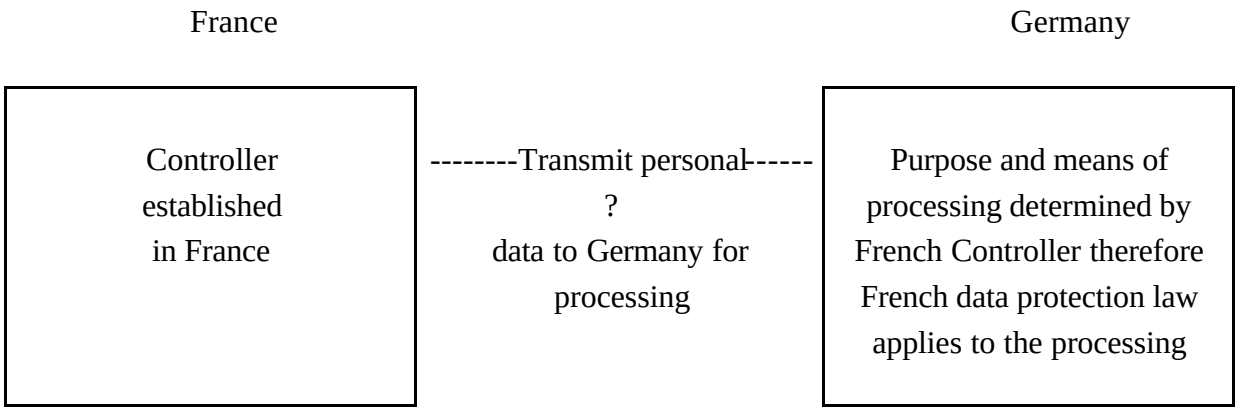
- introduce procedures for responding to requests from data subjects for rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the Controller's legitimate purposes.

3.3 Applicable national law - Article 4

3.3.1 Scope

Under the Directive, Controllers are subject to the law of the Member State where they are established (Article 4.1). Where a Controller is established in a number of Member States, the law of each of those Member States will apply to the Controller established in that territory. Where a Controller is not established in any Member State, the national law of a Member State may apply by virtue of public international law (Article 4.1(b)). Controllers not established in any Member State will be subject to Member State law where they make use of equipment, automated or otherwise, situated on the territory of a Member State unless the equipment is used only for the purposes of transit through the territory of the Member State (Article 4.1(c)). In this latter case the Controller must designate a representative established in the territory of that Member State though this will be without prejudice to any legal action which may be taken against the Controller personally (Article 4.2). Recital 18 explains what law is applicable when a Controller is established in one Member State but causes processing to be carried out in another Member State. The law of the original Member State will apply to such processing.

Figure 1: Operation of Article 4



3.3.2 Operational requirements

- Organisations must identify the Member States in which they have Controllers.

- Where a Controller is established in a third country, and equipment is used merely for the onward transit of the data, that is not sufficient of itself to make the law of the Member State in which the equipment is located applicable, but it does not absolve the Controller from designating a representative established in that Member State.

- Organisations must decide whether the circumstances set out in Recital 18 apply to them. That is, does the Controller established in one Member State cause processing to be carried out in another. If this is so, the law of the first Member State will apply to the processing in the second Member State.

  The implementation of the Directive will clarify the question of what law is applicable as well as introducing a level of similarity in those laws. This should lead to cost savings.

  However, the fact that Member States have a margin for manoeuvre in their implementation of the Directive means that Controllers may need to familiarise themselves with the laws in several Member States.

3.3.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers should identify the Member States where they are established and where they carry out processing. They should monitor the implementation of the Directive in those countries, paying particular attention to those provisions which allow Member States some discretion as to their implementation; and

- Controllers may consider applying the standards applicable in the Member State with the highest standards to their processing in all Member States.

3.4 Principles relating to data quality - Article 6

3.4.1Scope

The data quality principles in Article 6 are broadly derived from the Council of Europe's Convention on Data Protection. The principles require that personal data should be (Article 6.1) :

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes; and not further processed in a way incompatible with those purposes;

(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 that 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 were further processed.

Under the Directive, it is the Controller who is charged with the responsibility of ensuring that the data quality principles are complied with (Article 6.2).

3.4.2 Operational requirement

- Controllers must ensure that they comply with the five principles;

- Controllers will have to familiarise themselves with the implementing legislation on appropriate safeguards for historical, statistical or scientific use of data under Article 6. 1 (b) and (e);

- Controllers will have to observe the principles relating to data quality for manual filing systems as well as automated systems;

- Controllers must observe the principles relating to data quality regardless of the fact that they have received no complaints from data subjects. These are absolute standards.

The five data quality principles are already familiar in most of the Member States. What is new however is that the principles are now mandatory in all Member States, and that the obligation for ensuring compliance with the principles rests on the Controller. This means that the Controller must be satisfied that any activities carried out for him by a Processor are done in accordance with these principles.

3.4.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical step :

Controllers must review their processing complies with the data quality principles. A term must be incorporate in the relevant contract to this effect. This should be backed up by an indemnity clause. A suitable clause should contain all or some of the following elements :

"The Processor shall indemnify the Controller against all costs (including legal costs), claims, damages, demands and expenses arising directly or indirectly out of any breach of Article 6 of the Directive which arises in connection with [section x of the Data Protection Law]. »

3.5 Criteria for making data processing legitimate – Article 7

3.5.1 Scope

Article 7 details the situations where personal data may be processed. Personal data may not be processed if the processing does not fall within one or more of the provisions of Article 7.

3.5.2 Operational requirements

Prior to processing, Controllers should first determine which section of Article 7 is applicable.

Article 7 allows processing of personal data where one of a list of criteria are satisfied. For private sector organisations, these will frequently be Article 7(a) (consent) and Article 7(b) (performance of a contract) or in some cases, Article 7(f) (legitimate interests of Controller), with Article 7(d) (vital interests of data subject) and 7(e) (public interest) being applicable in very limited circumstances. The processing carried out by public sector organisations may fall within Articles 7(c) (Controller's legal obligation), (d) and (e).

3.5.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers will need to become familiar with the sub-sections of Article 7 prior to carrying out any processing, and will have to take a legally reasoned view as to the section of Article 7 that legitimises that processing. Where technically possible, data should be "marked" with the relevant section of Article 7. Where this proves difficult for historic data, organisations should consider marking new data.

- More specifically, Controllers will need to take the following steps in relation to the individual sections of Article 7:

    - Article 7(a), ensure that the data subject's consent has been properly acquired. This may for example require changes to the Article 10 Notice (see below);

    - Article 7(b), identify the contract being relied upon;

    - Article 7(c), identify the legal obligation which forms the basis of the processing;

    - Article 7(d), identify the vital interests of the data subject and on what basis the processing is necessary;

    - Article 7(e), identify the official authority and in each case ensure the processing is necessary;

    - Article 7(f), identify the legitimate interests, ensure that the fundamental rights and freedoms of the data subject are not overridden and ensure that all processing is necessary.

3.6 The processing of special categories of data - Article 8

3.6.1 Scope

Article 8.1 prohibits the processing of "sensitive data" i.e., data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life of individuals. The Article also lays down the exceptions to this general prohibition (Article 8.2). These are:

(a) where the data subject has given his/her explicit consent to the processing of those data; or

(b) where processing is necessary for the purposes of employment law in so far as it is authorised by national law which provides adequate safeguards; or

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

(d) where processing is carried out by a foundation, association or any other non-profit-seeking body with a political, philosophical, religions or trade-union aim, in the course of its legitimate activities, with appropriate guarantees, 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/have been made public by the data subject; or

(f) where the processing is necessary for the establishment, exercise or defence of legal claims.

Other exceptions include:

- health purposes (Article 8.3). 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, provided that the data are processed by a health professional subject to national law or rules established by national competent bodies with the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;

- public interest (Article 8.4). Member States may lay down additional exemptions based on substantial public interest subject to the provision of suitable safeguards.

Examples of the type of exemptions envisaged here are given in Recital 34. Such exemptions relate to benefits and services in respect of health insurance, scientific research and government statistics;

- data relating to offences, criminal convictions or security measures (Article 8.5). Such data may be processed only by or under the control of official authority. This is 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 (Article 8.6).

Article 8.7 requires a Member State to determine the conditions under which a national identification number or any other identifier of general application may be processed.

3.6.2 Operational requirements

- Controllers will have to become familiar with the concept of "sensitive data";

- Controllers must analyse their data and decide whether any item falls within the special categories set out in paragraph 1 of Article 8;

- if this is the case, Controllers must then examine whether any of the exemptions provided for in the Article applies to each item of sensitive data;

- Controllers must ensure that they fulfil all of the requirements of the relevant exemptions;

- if the medical or healthcare exemptions are to be relied upon, Controllers should review contracts of employment and contracts with independent contractors to ensure that they contain equivalent confidentiality clauses to those imposed on health professionals.

- Controllers must verify whether they obtained the data subject's consent in the prescribed manner;

- Controllers must check whether it is forbidden by national law to process such data notwithstanding consent.

Article 8 prohibits the processing of sensitive data subject to various exceptions.

3.6.3 Compliance

This provision should not have a major impact as many Controllers do not collect sensitive data in the ordinary course of their businesses. However, Controllers should be aware that they could have a limited amount of sensitive data on some files and in particular on employee files which may include, for example, information on employees' health, racial origin and membership of trade unions. Further, care should be taken where the information held may be sufficient to *reveal*[3] sensitive data. For example, an individual's name and place of birth, information commonly held on employee files, may reveal ethnic or racial origin.

In most cases, the processing of sensitive information regarding employees will not prove problematic as it is covered by one of the exceptions to the general rule including where the data subject has given his unambiguous consent (Article 8.2(a)). To ensure compliance with the Directive, employer/Controllers should ensure that they have the employee's consent. To this end, a suitable clause should be inserted in the contract of employment. Other exceptions of interest to employers are: Article 8.2(c) which applies where the data subject is physically or legally incapable of giving his consent and would appear to cover situations such as medical emergencies; and Article 8.2(b) which covers data required for employment law purposes.

Some data users, in particular those in the public sector such as health care providers and local authorities, process sensitive information as part of their everyday business. In such cases, the processing will usually be permitted under Article 8.2(a) or (c), or Article 8.3 (health purposes).

Private sector bodies such as insurance companies will find themselves particularly affected by the operation of Article 8.5 which severely limits the processing that can take place in respect of criminal convictions. Only if Member States have chosen to include derogations under specific safeguards may such processing occur.

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers should familiarise themselves with the concept of "sensitive data" and consider whether any of the data which they process falls within the definition;

[3] Article 8 states that Member States shall prohibit the processing of personal data *revealing* racial or ethnic origin, etc.

- Controllers who do process sensitive data must become familiar with the situations in which they may continue to do so as laid out in the Directive or implementing legislation. Controllers must ensure that they fulfil all of the requirements of the relevant exemptions which will in some cases be a complicated exercise;

- where Controllers are satisfied that their processing of sensitive data comes within one of the exemptions, this fact should be "recorded" on the data base if at all possible. Where, for example, the Controller is relying on Article 8.3, (s)he should review contracts of employment and contracts with independent contractors to ensure that they contain equivalent confidentiality clauses to those imposed on health professionals;

- employer/Controllers should ensure that they have the employee's consent to the processing of personal data. To this end, a suitable clause should be inserted in the contract of employment, for example :

  "The Employee consents to the Employer processing his 'personal data" [as defined herein / in the employee handbook] for the "purposes of his employment" [as defined herein / in the employee handbook] with Z Limited".

3.7 Information to be given to the data subject - Article 10

3.7.1 Scope

There are two instances under the Directive where data must be given to the data subject. These are:

- on the collection of personal data from the data subject (Article 10);

- where the data has not been collected from the data subject (Article 11).

Under Article 10, the data subject must be informed of :

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

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

Other information that must be given to the data subject where necessary “to guarantee fair processing” includes (Article 7.1 (c)) :

- 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.

3.7.2 Operational requirements

3.7.2.1 General comments

- Controllers have to distinguish between instances of data collected from the data subject and data collected from another source;

- Controllers now have to decide whether data subjects already know the information rather than that they ought to know the information or could reasonably be expected to know the information.

3.7.2.2 Operational steps

- Consider which further information is required and consider whether this information is necessary to guarantee fair processing and re-design forms accordingly;

- identify which information is voluntary and which information is obligatory and re-design forms accordingly;

- review all data protection notices (e.g., "fair collection notice"), and re-draft wording;

- Controllers will have to ensure that all data processing carried out under Article 10 is properly recorded.

Informing data subjects in accordance with Article 10 on the collection of data from the data subject should not be onerous because of the direct link with the data subject at this time.

The information can be given orally (including over the telephone), or written in a special notice. In some cases more than one medium of communication may have to be used to satisfy the Directive's requirements - for example, a "flash" notice on Direct Response Television may have to be followed up at a later time by further oral or written information. However it is done, as a general rule, the information should be given to the data subject as

early as possible in the relationship and preferably at the first point of contact. This could be, for example, where a driver first applies for a driver card.

Whether the information is given orally or in a special written notice, Controllers will have to make use of a suitable script or statement. As many Controllers already use such scripts or written statements in compliance with existing law in the Member States, this should not be an onerous requirement. In most cases, it will be enough to review and reformulate the wording of the information to ensure that it covers all the information required under the Directive.

In the case of employees, the necessary information could be contained in the employment contract. Alternatively, the information could be contained in the job application form or in the employee handbook.

It should be borne in mind that not providing sufficient information when the information is being collected from the data subject may require further information to be given to the data subject at a later stage (see Article 11). It must be emphasised that the failure to give sufficient information at the time of collection could have serious consequences for the organisation. Firstly, the value of the information collected may be greatly reduced. The information may be unusable for the purposes for which it was originally collected and therefore business plans of the organisation may be jeopardised. Secondly, if a further data protection notice has to be given, a mailing to all individuals on a database is an extremely costly exercise. For this reason, the initial Controller should consult with possible recipients of the data regarding exactly what information should be given to the data subjects at the time of first collection. Because of the existence of the requirements for the Article 11 notice, the Article 10 notice assumes a much greater importance since an effective Article 10 notice may render an Article 11 notice redundant.

3.7.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers will have to adopt the necessary technical and/or administrative means to distinguish between instances of data collected from the data subject and data collected from another source;

- Controllers will have to take a view as to whether data subjects already have the information - the fact that they ought to have the information or could reasonably be expected to have the information does not exempt Controllers from compliance;

- Controllers will have to review all data protection notices to ensure that they contain the information specified in Article 10 including:

- the identity of the Controller and his representative, if any;

- the purposes of the processing for which the data are intended;

- 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.

  - consider which further information is required and consider whether this information is necessary to guarantee fair processing and re-design forms accordingly. This could be the case, for example, where the personal data is to be disclosed or processed in a manner which would not be immediately apparent to the data subject - although individuals would not expect to be told that the data will be disclosed to and processed by the Controller's employees if the data are to be sold on for commercial purposes, this fact should be mentioned at the time of collection of the data and the data subject given the opportunity to object.

The following paragraphs provide a sample of the type of information that should be included in an Article 10 Notice[4]:

« XYZ Limited will hold the information you have given on this application form for administering your account, credit risk assessment and marketing. Your information will be disclosed to employees of these departments. We may pass your information to carefully selected organisations who may contact you by mail or by telephone with offers of goods or services. If you do not wish your information to be used for marketing purposes, please tick this box 6. You may apply for a copy of the information that we hold about you and you have the right to have any inaccuracies corrected.

PART A

[4] Additional information may be required where data is to be transferred to third countries - see Sections 3.18 and 3.19.

You must give the information required in Part A of this form to enable us to provide you with the goods or services you have requested.

PART B

In order to provide you with the best possible service, we would be grateful if you would answer the questions set out in Part B of this form. However, feel free to ignore any question that you do not wish to answer.

- Controllers will have to ensure that all data processing carried out under Article 10 is properly recorded.

- Controllers should ensure that their contracts with employees contain the appropriate Notice. The following paragraph gives a sample clause for inclusion in the employment contract:

  XYZ Limited maintains and processes personal data relating to its employees for the purposes of employment administration and pensions administration. The data are obtained from the employee directly, from the [tax authorities], the [social security body] and other statutory and public bodies. The data will be disclosed to employees and agents of XYZ Limited for the purposes stated. You have rights of access and rectification in relation to your personal data. Contact the Personnel Department for further information".

- Controllers should consider whether personal data is to be passed to third parties. If so, Controllers should consider whether they can provide the information required by Article 11 in the Article 10 notice so that there is no need for the second recipient of the information to provide the Article 11 notice. This will ensure substantial cost savings for second recipients and, so long as data subjects have all the information they require to be fully informed, there is no detriment to data subjects in combining the Article 11 notice with the Article 10 notice. Of course, this can only be done if the disclosures to the second recipients are in the contemplation of the Controller at the time when the personal data is collected.

3.8 Information where the data have not been obtained from the data subject - Article 11

3.8.1 Scope

Article 11 covers the situation where the data were not obtained from the data subject. Article 11(l) provides that the data subject must be informed either at the time the data are recorded,

or if disclosure to a third party is envisaged, no later than the time when the data are first disclosed to that third party as to:

(a) the identity of the Controller and/or his/her representative, if any;

(b) the purposes of the processing.

Other information that must be given to the data subject where necessary "to guarantee fair processing" includes (Article 11.1 (c)) :

- the categories of data concerned;
- the recipients or categories of recipients; and
- the existence of the right of access to and the right to rectify the data concerning him.

Under Article 11(2), there is an exception from the duty to inform the data subject on recording or disclosure, in particular for processing for statistical purposes or for the purposes of historical or scientific research, where the provision of such information proves impossible, or would involve a disproportionate effort, or if the recording or disclosure is expressly provided for by law. Member States are required to provide appropriate safeguards in these cases.

3.8.2 Operational requirements

- Controllers should identify the sources from which data are obtained to enable them to consider whether an Article 11 or an Article 10 notice applies;
- Controllers should consider the medium of the information and how the fair collection notice will be presented;
- Controllers should decide whether their activities fall under Article 11 (2) and on what basis. Do their activities involve an impossibility or disproportionate effort?
- some of the implications of Article 11 for Controllers may not be immediately obvious:
    - where a Controller collects data from a primary collector of information, who has already informed the data subject of the disclosure to that Controller, is the data subject held to already have the relevant information, or does (s)he need to be informed again in order to comply with Article 11?

The answer to this question would appear to be that there is no need for an Article 11 notice when the data subject is already aware of the information that would be required under that provision in particular, the identity of the new Controller;

- in accordance with the Article, the time by which an Article 11 notification must be given depends on the Controller envisaging or not envisaging a disclosure of the data to a third party. If a disclosure to a third party was envisaged but no such disclosure ever took place, is the processing of the data still fair for those purposes which do not involve any third party disclosure? The answer to this question would appear to be that processing continues to be fair as long as disclosure is envisaged in the Article 10 notice. This must be the purpose of the processing operation.

Article 11 introduces a new requirement into the law of many Member States. It requires that information must be given to the data subject :

- where personal data which have not been obtained directly from the data subject are recorded; or

- where personal data which have not been collected from the data subject are disclosed to a third party, whether or not this disclosure was envisaged when the data were first collected from the data subject.

An important point for Controllers to take into account is that the data need not be given when the data subject already has it. This means that where disclosure to a third party is envisaged at the time of collection of the information from the data subject (the Article 10 situation) it may be possible to give the necessary information covering a further foreseen disclosure at this time. This fact makes it of the utmost importance for the initial Controller to consult with possible recipients of the data in order to decide exactly what information should be disclosed to the data subject when the information is being collected from him or her. Whether or not this has been done will have serious implications for the subsequent value of the data and for the costs of the second Controller. Controllers who obtain information from sources other than the data subject should consider the contracts under which this information is obtained and amend these contracts to reflect the new requirements. These contracts should deal with the question of informing data subjects and should place the responsibility and the cost on the first Controller as original collector of the personal data.

There is a minor difference in the requirements under Articles 10 and 11. The further information in Article 11 requires the categories of data intended to be disclosed to the third party to be described when it is necessary to guarantee fair processing. It would appear that

this is only required where parts only of the data are to be transmitted to the third party and not the whole.

3.8.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- as is the case with Article 10, it is important that Controllers have the administrative and technical means to record properly the source of the data i.e., whether it comes from the data subject (Article 10), or from another source (Article 11);

- where the information is not obtained from the data subject, the Controller will have to consider whether the data subject needs to be informed and when this should take place;

- Controllers will have to take a legally reasoned view as to whether data subjects already have the information - the fact that they ought to have the information or could reasonably be expected to have the information does not exempt Controllers from compliance;

- Controllers should prepare a data protection notice for use in connection with Article 11;

- Controllers should consider the contracts under which they obtain information from parties other than the data subjects and amend these contracts to reflect the new requirements. These contracts should deal with the question of informing data subjects. This will have serious implications for the value of the data.

Controllers should decide whether some or all of their activities could benefit from the exception established in Article 11.2 (disproportionate effort). Matters to be taken into consideration in considering disproportionate effort could include the number of data subjects. Controllers who operate databases which contain information on all adults in a Member State must be able to avail themselves of the argument that to contact the entire adult population by mail would involve disproportionate effort. Controllers should also be aware of the appropriate safeguards that will be adopted by each Member State in their implementation of the Directive.

3.9 Subject access - Article 12

3.9.1. Scope

Under Article 12, Member States are required to give data subjects a right of access to the following information "without constraint and at reasonable intervals" (Article 12 (a)):

- confirmation as to whether or not data relating to him are being processed, the purpose 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 the source of the data; and

- 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(l).

The data subject also has a right to have data rectified, erased or blocked if the processing is contrary to the provisions of the Directive and in particular where the information is either incomplete or inaccurate (Article 12(b)). Unless it proves impossible or involves a disproportionate effort, third parties to whom such data have been disclosed should be notified (Article 12(c)).

3.9.2 Operational requirements on Controllers

Controllers will have to re-design their subject access procedures to include the further information required by the Directive;

- Controllers will have to either ensure that they are in a position to notify third parties to whom the data have been disclosed of any rectification, erasure or blocking or put procedures in place which prove that this activity is impossible or adduce evidence that the effort would be disproportionate;

- Controllers will need to begin recording their data sources and the organisations to whom they have disclosed data;

- Controllers are required to communicate the data to the data subject in an intelligible form;

- Controllers must be prepared to respond to data subject's requests for information without excessive delay.

The law of many Member States already makes some provision for subject access to personal data. Despite this fact, such requests remain minimal throughout the European Union and it is not expected that the Directive will lead to a significant increase.

In the past some Controllers have taken the view that there was no point putting proper subject access mechanisms in place because of the small amount of requests. However, in preparing for the implementation of the regulation (EC) n° 2135/98 into national law as regards the Directive, Controllers should pay particular attention to the following points:

- the fact that subject access requests will now extend to manual files could pose problems for Controllers holding large amounts of information on manual files especially where such files are dispersed throughout the Controller's organisation, in different departments and indeed sometimes in different Member States. In this context it should also be noted that the possible exemption from certain provisions of the Directive for up to 12 years for manual files does not apply to subject access; and

- the amount of information to which the data subject is entitled. In addition to accessing personal information, under the new law the data subject must be given information concerning the purpose of the processing, categories of data, recipients or categories of recipients and the logic involved in any automated decision systems.

If proper mechanisms are not put in place, the costs of compliance in the scenario outlined above (manual files dispersed throughout an organisation) could soar. These costs should be passed on to the data subject as the Directive specifies that the information must be made available without excessive expense. Controllers could also find that they are unable to comply with the stipulation that the information should be made available without excessive delay.

Some Controllers may be worried by the prospect of having to provide "knowledge of the logic" involved in automatic processing. However, Recital 41 to the Directive emphasises that the right to know must not adversely affect intellectual property rights including trade secrets provided that this does not result in the provision of no information whatsoever. The techniques, and also the criteria, used in automated decision making are likely to be covered by this provision. It should also be borne in mind that one of the exceptions to subject access which a Member State can opt for is the prevention of criminal offences. This implies that in situations where providing knowledge of the logic raises legitimate concerns, it should be sufficient that the Controller give data subjects a broadly phrased response or, where the situation is covered by a clear exemption, no response on this point at all.

The Directive states that data subjects have the right to obtain from the Controller as appropriate the "rectification, erasure or blocking of data". In this context "blocking" means retaining the information but preventing it from being processed further. This is sometimes

known as suppression. The fact that some data is to be blocked can be "flagged" on the database.

Because of the very wide definition of processing in the Directive which includes every activity from selection to destruction, Article 12 on the right of access could have serious hidden cost consequences for Controllers since they will have to grant subject access rights to data which has been archived. There are many reasons, including compliance with national law, why public and private sector organisations should hold archived data for many years. Because such information may not be of immediate relevance to the business or public sector activities of the organisation, it may be archived and kept in a format which is not immediately available to satisfy subject access requests without at least some cost consequences. These could include the cost of operators' time in searching the index of the archive site in order to identify the information, physical retrieval of the information from the archive site, transport of the information from the archive site to a place where it can be processed and, finally, the processing of the information in order to retrieve the necessary information to satisfy a subject access request. It can be seen that when these activities are added together, the cost is sometimes quite high.

3.9.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers will have to re-design their subject access procedures to include the further information required by the Directive, namely; the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the data are disclosed, information as to the source of the data and knowledge of the logic involved in any automatic processing of data concerning the data subject;

- Controllers will have to either ensure that they are in a position to notify third parties to whom the data have been disclosed of any rectification, erasure or blocking or put procedures in place which prove that this activity is impossible or adduce evidence that the effort would be disproportionate;

- Controllers will need to begin recording their data sources. Though the Article only says "any available information as to the source of the data", it may in time become the practice for Controllers to indicate their sources of information;

- Controllers are required to communicate the data to the data subject in an intelligible form;

- Controllers must be prepared to respond to data subject's requests for information without excessive delay; and

- Controllers may consider fully automating their subject access procedure.

3.10 The data subject's right to object - Article 14

3.10.1 Scope

Under Article 14, Member States must grant data subjects the right to object to the lawful processing of personal data "on compelling legitimate grounds relating to [their] particular situation" where the processing is carried out under Article 7(e) or Article 7(f) (public interest and the legitimate interests of the Controller) "save where otherwise provided by national legislation" The processing may no longer involve the data where there is a "justified objection" (Article 14(a)). Member States must also grant data subjects:

- the right to object, on request and free of charge, to the processing of personal data which the Controller anticipates being processed for the purposes of direct marketing (Article 14(b), though some Member States may grant data subjects the right to object in other cases as well); or

- the right 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 (Article 14(b)).

3.10.2 Operational requirements

- Although this Article is addressed to Member States, Controllers will have to inspect the relevant implementing legislation and ensure that they provide to data subjects the rights set out in this Article;

- Controllers will have to put procedures in place to suppress or block data when requested so to do by data subjects;

- Although the final paragraph is addressed to Member States, presumably, the measures mentioned will be enshrined in legislation and Controllers will have a duty placed upon them to ensure that data subjects are made aware of the existence of the rights referred to in the first sub-paragraph of (b).

3.10.3 Compliance

Although this Article is addressed to Member States, Controllers will have to inspect the relevant implementing legislation and ensure that they provide data subjects with the rights set out in this Article. As a practical step, Controllers will have to put procedures in place to suppress or block data when requested so to by data subjects. However, the Controller must also have procedures in place to ensure that such requests are "justified" where the Controller is processing on legitimate grounds.

The suppression or blocking of data, at least for direct marketing purposes, will not add any additional cost, at least for Controllers based in Member States where requirements very similar to the Directive are already in place or where self-regulation in the direct marketing industry already provides for such suppression.

3.11 Automated individual decisions - Article 15

3.11.1 Scope

Paragraph 1 of Article 15 prohibits automated decisions by granting the data subject the right not to be subject to a decision which produces legal effects or significantly affects him and which is based solely on automated processing of data intended to evaluate certain of personal aspects such as performance at work, creditworthiness, reliability and conduct etc. The list of personal attributes is not exhaustive. Paragraph 2 lists exceptions to this general principle. These are where such a 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 a law which also lays down measures to safeguard the data subject's legitimate interests.

3.11.2 Operational requirements

- Controllers must review their business systems to identify those which include entirely automated decision making;

- Controllers should consider whether to introduce a human element in those which are entirely automated;

- Controllers should put in place appeal procedures to allow individuals to put their points of view;

- if certain automated decision making processes are to be authorised by national law, Controllers should familiarise themselves with the procedures required.

This Article prohibits decisions made solely by automated means. It is enough that there is some human input into the decision making process to take the process outside the scope of the prohibition. However, the human input must be a real contribution to the decision making process. It is not enough, for example, that a human operator merely presses a button or rubber stamps what is otherwise an automated decision.

The prohibition against automated decision making is not absolute. The Directive makes clear that it will not apply to situations where it is the data subject who wishes to enter into a contract and either his/her request is accepted or, where the request is rejected, there are suitable safeguards to satisfy his/her legitimate interests, such as arrangements for letting him/her put across his/her point of view. This would appear to cover the situation where the data subject goes into a retailer and applies to buy goods on credit. If (s)he is accepted as a good credit risk following an automated credit check, then well and good, if not, (s)he must be able to put his/her views across. The Directive is silent on how this should be done. However, there are existing examples which could be of use in these circumstances. For example, the data subject could be given the telephone number of the credit checking agency so that if (s)he has been turned down for credit, (s)he may telephone to find out why, and have the opportunity of putting his/her point of view immediately. The data subject may be asked in such a telephone conversation to provide further information which could assist the application for credit. The commercial incentive on the credit grantor is always to increase the numbers of individuals to whom (s)he grants credit since this increases his/her profit. No retail organisation is in the business of turning down reasonable applicants who wish to buy its goods or services.

3.11.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps :

- Controllers must review their business systems to identify those which include entirely automated decision making;

- Controllers should consider whether to introduce a human element in those which are entirely automated;

- Controllers should train staff to deal with situations under Article 15(2) where the data subject's request has not been accepted;

- Controllers could consider putting in place appeal procedures to allow individuals to put their points of view;

- If certain automated decision making processes are to be authorised by national law, Controllers should familiarise themselves with the procedures required.

3.12 Confidentiality of processing - Article 16

3.12.1 Scope

This Article provides that any person acting under the authority of the Controller or of the Processor, including the Processor him/herself, who has access to personal data, must not process them except on instructions from the Controller, unless (s)he is required to do so by law.

3.12.2 Operational requirements

Controllers will have to specify the limits of the processing in the written contracts that they use with Processors, agents or independent contractors. If this is not done, the Processor, agent or independent contractor may require an indemnity from the Controller to cover the risk of liability or they may refuse the appointment.

This Article is of importance to Processors as well as Controllers as it underlines that Processors, their employees and agents must process personal data only in accordance with the Controller's instructions. An exception is where the processing is required by law. This could be the case, for example, where the processing is a necessary part of a criminal investigation.

3.12.3 Compliance

To ensure cost effective compliance with this Article, Processors and Controllers should take the following practical steps:

- processors should ensure that they have formal written instructions from the Controller. They must communicate these instructions to any employees and agents who have access to the personal data being processed. Processors should consider

restricting access to the data. This could be done, for example, by the use of personal passwords; and

- on the other hand, Controllers should take the opportunity to review their contracts with Processors, agents or independent contractors. These contracts should spell out the authority granted to such persons. Where this is not done, the Processor, agent or independent contractor may require an indemnity from the Controller to cover the risk of liability or they may refuse the appointment.

  A suitable clause could contain the following elements:

  1. *A Limited undertakes to be bound by the acknowledges that it has been made fully aware of the provisions of [Member State] Data Protection Law, hereinafter referred to as "Data Protection Law", particularly sections xx and xx. This Agreement in its entirety is subject to such Data Protection Law and these terms and provisions shall have the meanings assigned to them in the Data Protection Law.*

  2. *A Limited recognises that all* [insert description of the relevant 1 data] *(the "Data") Data is confidential in nature and therefore in consideration for Data being communicated by B Limited to A Limited, A Limited undertakes that unless prior written consent is obtained:*

     (1) *it shall process the Data disclosed to it exclusively for the purposes reflected in Schedule 1 attached and for no other purposes whatsoever;*

     (2) *it shall process the Data communicated to it strictly in accordance with the specific instructions of B Limited;*

     (3) *it will not publish, disclose or divulge or disseminate Data to any third party under any circumstances whatever;*

     (4) *it shall procure that each of its employees will be informed of the confidential nature of the Data and shall sign the Confidentiality Declaration attached as Schedule 2 before being granted access to the Data, and then shall handle the Data strictly on a need-to-know bases. Such Confidentiality Declaration shall endure for the duration of this Agreement;*

     (5) *it will take all technical and organisational measures necessary in order to secure the confidentiality of the Data. To this end the requirements of Data Protection Law shall be used as a minimum guideline for such protective*

measures, provided however that A Limited shall also undertake not to transmit in any form or by any means whatsoever the Data outside its usual place of business, and A Limited shall upon B Limited's request immediately deliver to B Limited all disks and the like in its possession, custody and control, that include or relate to the Data and shall not retain any copies thereof in any computer or electronic retrieval system;

(6) *it will, at B Limited's request, allow the data protection officer nominated by B Limited, access to the premises occupied by A Limited. A Limited shall provide such officer with information and documentation necessary for the performance of his duties and shall furthermore follow his recommendations if he suggests that measures be taken to rectify technical and/or organisational irregularities;*

(7) *it shall inform B Limited immediately of any suspicion regarding a violation of Data security. The security representative of B Limited shall have the right to conduct checks at the premises of A Limited in order to satisfy itself of A Limited's adherence to this Agreement.*

3.13 Security of processing - Article 17

3.13.1 Scope

Article 17 imposes obligations on Controllers in respect of security of data providing that the Controller must take appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, in particular where the processing involves the transmission of data over a network. Having regard to the state of the art and cost, the measures taken must ensure a level of security appropriate to the risks represented by the processing and the nature of the data that it is sought to protect (Article l7.1).

The Article also requires Controllers to choose Processors who can provide sufficient guarantees in terms of technical security measures and organisational measures (Article 17.2). Further, the processing carried out by a Processor must be governed by a contract or legal act binding the Processor to the Controller. Such contract or legal act must provide that:

- the Processor shall act only on instructions from the Controller;

- the obligations placed on the Controller are also incumbent on the Processor (Article 17.3).

For evidential purposes, 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 (Article 17.4).

3.13.2 Operational requirements

- Where the Controller intends to transmit data over a network, this Article may impose an additional requirement on Controllers to implement technical and organisational measures over and above what would otherwise be required;

- Controllers must demonstrate that their security measures have been chosen by reference to their appropriate nature;

- Controllers must choose Processors carefully and must draft contracts to comply with all the new requirements in Article 17. In addition, paragraph 2 may require them to enforce such contracts. Controllers will have to develop closer relationships with Processors than is currently the case. Those who fall under the definition of Processor must train their staff and reorganise their management structures to take account of the greater risk they are assuming under the Directive.

Under this Article, Controllers are obliged to take security measures to protect personal data. These security measures must be appropriate to the risks represented by the processing and the nature of the data to be protected.

3.13.3 Compliance

The requirements of this Article largely reflect good information technology management and for this reason, many Controllers will find that they already comply. For Controllers that are not already in this happy position, the implementation of the Directive and of the regulation (EC) n° 2135/98 should be seen as an opportunity for a full scale review of security measures. All controllers should bear in mind that the provision will also apply to manual files.

Controllers should ensure that employees dealing with personal data are aware of the security provisions of the Directive. This will involve training. Controllers should also consider providing written guidelines to employees on security issues. These could cover, for example:

- the correct use and security of passwords;

- the importance of limiting access to personal data by, for example, logging out of the system when the information is not in use or the computer is not being attended by the authorised employee;

- the secure storage of manual files, printouts, computer floppy disks;

- the operation of a clean desk policy;

- a general prohibition on removing personal data from office premises;

- the proper disposal of confidential data by shredding, etc…

Staff should also be made aware of any special risks associated with their particular activities. For example, some retailers use screens displaying customer information at points of sale. Controllers should instruct staff to ensure that the display screen cannot be read by other customers.

Controllers must ensure that external processors also satisfy the requirements of this Article. To ensure that this is the case, the Controller should check and evaluate all the flows of information to outside organisations (computer bureau, other processors), as well as other companies in the same group, and ensure that the existing arrangements contain the appropriate contractual terms. Controllers using networks must ensure that data is only transmitted when the appropriate security measures are in place.

Controllers have a two year transitions period before the introduction of the regulation (EC) n° 2135/98 (in practise reduced to few months due to the necessity to issue driver cards 21 months after the date of publication of the technical specifications of the digital tachograph – 5 August 2002) in order to bring their security measures into line with the provisions of the Directive. This two year period also applies to manual records.

To ensure cost effective compliance with this Article, Processors and Controllers should take the following practical steps:

- Controllers should check and evaluate all the flows of information to outside organisations and ensure that the existing arrangements contain the appropriate contractual terms;

- Controllers should ensure that employees dealing with personal data are aware of the security provisions of the Directive, training staff accordingly;

- where the Controller intends to transmit data over a network, this Article may in some circumstances impose an additional requirement on Controllers to implement technical and organisational measures over and above what would otherwise be required. Although there is no express mention of encryption in the Directive, in certain circumstances this may be a requirement;

- Controllers must demonstrate that their security measures have been chosen by reference to their appropriate nature. Controllers must keep the state of the art of security measures under review to ensure that what was once appropriate continues to be so;

- Controllers must choose Processors carefully and must draft contracts to comply with all the new requirements in Article 17. In addition, paragraph 2 may require them to enforce such contracts. Controllers will have to develop closer relationships with Processors than is currently the case. Those who fall under the definition of Processor must train their staff and reorganise their management structures to take account of the greater risk they are assuming under the Directive.

The clauses set out under paragraph 3.12.2 are relevant to this section as well.

3.14 Obligation to notify the supervisory authority - Article 18

3.14.1 Scope

In compliance with Article 18, Member States must provide that the Controller or his representative should notify the Supervisory Authority before carrying out any wholly or partly automatic processing operation, or set of such operations which are intended to serve a single purpose or several related purposes.

Under Article 18.2, Member States may provide for simplification of or exemption from the notification requirements where:

- the rights and freedoms of data subjects are unlikely to be adversely affected by the processing;

- where Controllers in compliance with national law, are required to appoint a personal data protection officer charged with ensuring compliance and with keeping a register of processing operations;

- in the case of public registers (such as the electoral roll),

- processing operations referred to in Article 8.2(d) (voluntary and other similar organisations).

3.14.2 Operational requirements

- Controllers must identify all processing operations which are wholly or partly automatic and comply with all notification requirements except where an exemption is allowed;

- if a representative is required to be designated in a Member State in which the Controller is not resident, the Controller must ensure that the representative fulfils any local notification requirements if the Controller itself has not done so;

- in the case of non-automatic processing operations, Controller must identify which must be notified.

The notification requirement contained in this Article is not expected to be burdensome to Controllers. Indeed the implementation of this provision into Member State law should result in a lightening of the existing notification requirements in several Member States.

The general requirement to notify is subject to several important exceptions:

- where "the rights of data subjects are, unlikely to be adversely affected". In such cases, Member States are given the option of simplifying the notification requirements or exempting altogether from the requirement to notify. This provision may result in a large number of bodies (including many small traders and manufacturing companies), which do not process sensitive information being exempt from notification in the Member States that use this option. Charities and other non-profit making organisations should take note that processing of sensitive data may also be exempted in limited situations,

- manual files. The requirement only applies to wholly or partially automated processing. With regard to manual files, Member States are given the option either of simplifying the notification requirements or exempting such files altogether from the requirement to notify;

- the appointment of a data protection officer. Again, Member States are given the option either of simplification of the notification requirements or outright exemption from notification requirements in cases where the Controller appoints an independent data protection officer. The data protection officer would be responsible for ensuring both compliance with national law within the Controller's organisation and that the rights and freedoms of data subjects are not being adversely affected by the processing operations. Under the Directive, the data protection officer would also keep a register of processing operations carried out in the Controller's organisation.

Processors should note that the requirement to notify only applies to Controllers.

3.14.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers must watch the implementation of this Article into Member State law paying particular attention to the options chosen by the Member State in question with regard to:

  - notification requirements where "the rights of data subjects are unlikely to be adversely affected" by the processing operations;

  - notification requirements concerning the processing of manual files;

  - notification requirements in cases where the Controller has appointed a data protection officer.

- if a representative is required to be designated in a Member State in which the Controller is not resident, the Controller must ensure that the representative fulfils any local notification requirements if the Controller itself has not done so.

3.15 Contents of notification - Article 19

3.15.1 Scope

This Article, which is addressed to the Member States, sets out the type of information to be given in the notification by the Controller to the Supervisory Authority:

(a) the name and address of the Controller and of his/her 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 measure to be taken pursuant to Article 17 to ensure security of processing.

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 19.2).

3.15.2 Operational requirements

Controllers should prepare a general description of security measures relating to the processing of the data;

Controllers that are required to register must provide the information stipulated in this Article to the Supervisory Authority;

Controllers may be concerned by the requirement to give a description of measures taken pursuant to Article 17 to secure security of processing as they may rightly be concerned that their security could be compromised in some way. However, it would appear to be adequate fulfilment of this requirement to provide a generalised statement concerning security. Further, Controllers should take comfort from the fact that the register of notifications that will be kept by the Supervisory Authority and be open to public inspection will not include the information concerning security.

3.15.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- prepare a general description of security measures relating to the processing of the data. This should contain all of the elements included in the following paragraphs :

  1.1 The Processor shall maintain state of the art security measures to protect the integrity of information, make it available in a timely manner, and prevent disclosure to unauthorised parties. The Processor shall notify the Controller promptly of any breaches, whether realised or potential.

  1.2 Each party warrants to the other that it is properly registered under the Data Protection Law in respect of any personal data supplied or held under this

agreement and shall keep such registration current throughout its term, and shall notify any changes to its registration to the other party.

1.3 Each party shall comply with the principles set out in[appropriate standard]. Where communications connections are implemented between the parties to provide system access and/or to transmission of information, a technical annex shall set out the security principles and measures to be implemented by and between the parties to ensure the security of the connections

1.4 Detailed security measures to secure information being processed by the parties are expected to include measure for the security of :

1.4.1 telecommunications systems, with particular emphasis upon networking, remote access, Internet,

1.4.2 use of authentication systems including passwords, tokens, biometrics;

1.4.3 methods for monitoring and reporting security breaches and/or attempted security breaches;

1.4.4 disaster recovery, contingency planning and related activities;

1.4.5 user and management awareness, education and training in information security issues and matters including requirements of the Data Protection law;

1.4.6 use of encryption for the purposes of authentication, non-repudiation and preventing unauthorised disclosure of information;

1.4.7 detection and removal of viruses or other malignant computer codes or instructions.

3.16 Publicity of processing operations - Article 21

3.16.1 Scope

Under Article 21.1, Member States are directed to take measures to ensure that processing operations are publicised. In particular, they should provide that the Supervisory Authority keep a register of notified processing operations. This register is to contain at least the information listed in Article 19.1(a) - (e) (i.e., all information that must be provided on notification except that relating to security measures), and should be open to inspection by any person.

Member States are also directed to ensure that Controllers that are exempt from notification provide at least the information referred to in Article 19. 1 (a) to (e) to any person on request. However, 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.

3.16.2 Operational requirements

- Controllers must prepare statements of processing including proposed transfers of data to third countries and a general description of the security of processing.

- Presumably Controllers will be required to keep this statement up to date and it may well be part of the annual audit activities of auditors to a company to inspect the processing statement and to ensure that it covers all the current activities of the organisation.

- Controllers must put in place a system for receipts of requests for copies of the statement of processing so that these can be dealt with centrally and sent out in a timely fashion.

Under this Article, those Controllers that are not subject to the notification requirements must prepare and make available the information specified in Article 19.1 (a) - (e), in an appropriate form to any person upon request. It should be noted that the statement of security measures is not included under this requirement. Compliance with this requirement may also require some employee training.

3.16.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers must prepare statements of processing which must include the information required under Article 19 (a) - (e);

- Controllers should train relevant employees in how to respond to requests for information under this Article;

- Controllers will be required to keep this statement up to date and it may well be part of the annual audit activities of the auditors of a company to inspect the processing statement and to ensure that it covers all the current activities of the organisation;

- Controllers must put in place a system for handling requests for copies of the statement of processing so that these can be dealt with centrally and sent out in a timely fashion.

Controllers should note that there is no provision in the Directive for payment for a copy of the statement.

3.17 Liability - Article 23

3.17.1 Scope

Member States must 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 the Directive, is entitled to receive compensation from the Controller for the damages suffered (Article 23.1). The Controller can be exempted from this liability, in whole or in part, if (s)he can prove that (s)he is not responsible for the event giving rise to the damage (Article 23.2).

3.17.2 Operational requirements

Controllers may require their insurers to extend insurance coverage to include this liability. Under this Article, Controllers may have to provide compensation to data subjects who suffer damage as a result of an unlawful processing operation or an act that is incompatible with national law implementing the Directive. However, the Article goes on to provide that the Controller may be exempted from this liability in whole or in part if (s)he can prove that (s)he is not responsible for the event giving rise to the damage.

3.17.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical step :

- Controllers may require their insurers to extend insurance coverage to include this liability;

- Controllers should examine national law implementing this provision.

3.18 Transfer of information to third countries - Article 25

3.18.1 Scope

The basic principle laid down in the Article is that Member States must provide that the transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country, may only take place if that third country provides an adequate level of protection. This must be without prejudice to the provisions of the Directive, meaning that processing in the third country must comply with data protection law in the Member State from which the data is transferred (Article 25.1).

Article 25.2 provides a non-exhaustive list of the factors that should be taken into account in assessing the adequacy of the level of protection in the third country:

- all the circumstances surrounding a data transfer operation or set of data transfer operations;
- 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;
- the professional rules and security measures which are complied with in that country.

Under Article 25.3, 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. Where the Commission makes this finding in respect of a third country, Member States shall take the measures necessary to prevent any transfer of data to that country (Article 25.4). The Commission shall enter into negotiations with the third country with a view to remedying the situation at an appropriate time (Article 25.5). The Commission may also make a finding that a third country does provide an adequate level of protection (Article 25.6) and in such cases, Member States should again take the necessary measures to comply with the Commission's findings.

3.18.2 Operational requirements

- Controllers must identify the third countries to which they transmit or intend to transmit data undergoing processing or transmit personal data which are intended for processing in such a third country.

Many factors have led to an increase in transfers of information, including personal data, to third countries. These include the global nature of many businesses, the growth in telecommunications networks and the subsequent possibility of making use of processing facilities in other countries where input costs are lower. Where data which have been processed in a third country are subsequently to be used within the EU, the processing will be covered by EU law.

Controllers should be aware that once the Directive is in force, there could be restrictions or even prohibitions on transferring data to some third countries. This will be the case where, subject to various exceptions (see in this respect Article 26), that third country is not seen as having "adequate" protection.

How will a Controller know whether the country to which (s)he sends his data for processing has an adequate level of protection? According to the Directive, the matters that have to be taken into account in making this assessment include: the nature of the data; its purpose, duration, etc... Thus it is possible that a third country may have an adequate level of protection for some processing operations but not for others. It is also possible that the Member States will approach this problem in different ways. At this stage, there appear to be at least three options:

- the Controller him/herself takes the decision;

- the Controller takes the decision based on the guidance of the Supervisory Authority; and

- the Controller must get the authorisation of the Supervisory Authority prior to making any transfer.

It is suggested that interested Controllers watch developments on this point at national level.

3.18.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers must identify the third countries to which they transmit, or intend to transmit, data undergoing processing or to which they transmit personal data which are intended for processing, and conduct enquiries as to whether these countries are seen as ensuring an adequate level of protection.

3.19 Derogations from Article 25 - Article 26

3.19.1 Scope

Article 26 lists the situations in which 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. These are:

(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.

Further, a Member State may authorise a transfer or a set of transfers of personal data to a third country, which does not ensure an adequate level of protection, 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 (Article 26.2).

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.

3.19.2 Operational requirements

- Controllers must carry out an audit to identify the third countries to which they transfer or intend to transfer data;

- Controllers must inform themselves as to which countries provide an adequate level of protection and which do not;

- in the case of transfers to non-compliant countries, Controllers must ensure that their activities fall under one or more of the exemptions provided for in paragraph 1 of Article 26;

- alternatively, Controllers may draft appropriate contractual clauses to provide the safeguards required in paragraph 2;

- once the Commission has approved standard contractual clause wording, Controllers would be well advised to adopt such standard clauses;

- Controllers will be required to comply with national procedures in connection with the evaluation of the level of protection, this might include notification of data transfers abroad and in some circumstances, the obtaining of authorisations.

Where the third country does not have an "adequate level of protection", the data may be transferred subject to the conditions laid down in Article 26. It is up to the Controller to ascertain that these conditions have been satisfied.

Some of the conditions will prove very useful. They include:

- where the data subject has given his/her consent or the transfer is related to the performance of a contract;

- where the Controller adduces adequate safeguards.

This first condition will apply to many processing operations carried out by retail and financial institutions. To satisfy the second condition, the Controller will need to formulate appropriate contract conditions for inclusion in the contract with the processor. These should address such matters as:

- prohibitions on subsequent disclosure to others in third countries;

- minimum levels of security measures;

- require the return or verifiable destruction of data following the relevant operations.

Approved standard clauses for this use may also be formulated by the Commission.

3.19.3 Compliance

To ensure cost effective compliance with this Article, Controllers should take the following practical steps:

- Controllers must carry out an audit to identify the third countries to which they transfer or intend to transfer data;

- Controllers must inform themselves as to which countries provide an adequate level of protection and which do not;

- in the case of transfers to non-compliant countries, Controllers must ensure that their activities fall under one or more of the exemptions provided for in paragraph 1 of Article 26;

- alternatively, Controllers may draft appropriate contractual clauses to provide the safeguards required in paragraph 2.

Annex 1

Model for a data protection audit

DATA PROTECTION AUDIT

1. Purpose

The purpose of a data protection audit is to obtain as complete a picture as possible of the structure of the information flows within an organisation so that the correct compliance procedures can be put in place to ensure that the organisation deals with personal data in accordance with data protection law, the general law and best practice.

In small organisations nothing as complex as the following questionnaire needs to be used, although the questions set out below might be helpful in prompting the thinking of the person responsible for ensuring compliance with data protection law.

However, in complex organisations, particularly groups of companies with many devolved subsidiary companies or activities in dispersed locations, the procedure set out in this annex is essential.

2. Organisation Chart

For complex organisations the first stage is to obtain (or produce if one docs not already exist) an organisational chart showing the operational, managerial and departmental structure of the organisation together with the names and locations of the personnel who have managerial or operational responsibility for information within the organisation.

3. Questionnaires

Data protection audit questionnaires should then be sent to each named individual for completion or may be used as the basis for face-to-face interviews.

4. Analysis of information

Once all the questionnaires have been completed the organisation is in a position to compile a complete diagram of the use of information within the organisation, which can then form the basis of a review of the organisation's compliance with data protection law and other relevant law.

For complex organisations it is recommended that such audits are carried out annually.

5. Suggested data protection audit questionnaire

Name: Job title: Department: Location:

Collection

1. **<u>Does your department process personal data on:</u>**

individuals	?
sole traders	?
partnerships	?
companies	?

2. If so, who authorises the collection?

3. For what purposes is the information collected?

4. What information is collected?

5. How is the information collected? Is it collected face to face with the individual or at a distance?

   If face to face is collection:

by interview	?
in a retail outlet	?
by attendance at an event or of function	?

If collection occurs at a distance, is it:

an in-bound telephone call	?
an out-bound telephone call	?
via the internet website	?
a fax	?

In either case, is a paper format used such as an application form. Please attach examples.

6. From whom is the personal data collected:

individuals themselves	?
third parties	?
intermediaries, e.g. list brokers	?
financial advisers, joint venture partners	?

7. What form of data protection notice is given to individuals when the information is collected? Please attach copies.

8. How often is this notice reviewed or changed?

9. Who reviews or changes the notice?

Storage, Processing and Disclosure

10. Does your department store personal information? If so, is the storage:

on computer	?
in manual files	?
both on computer and manually	?

11. If storage of information is on computer, is this:

in-house	?
by third parties	?

12. If storage is on computer, where is it located?

13. What processing activities are carried out by your department?

14. Are any of your processing activities carried out by third parties? If so, please list them and describe the processes.

15. Who authorises these processing activities?

16. Who has authority to change, add or delete data?

17. Who has access to personal data? Please list?

within the organisation
outside the organisation

18. Who authorises such access?

19. Describe the manual filing storage system.

20. Do you consider that your department holds any sensitive data? If so, please describe the sensitive data and why it is held.

21. Do you disclose data to

Other departments in the organisation ?
Third parties outside the organisation ?

22. In what countries are those people to whom you disclose the information (whether inside the organisation or external) located? Please list.

Subject access procedures

23. Please describe the procedures in your department for supplying information in response to a subject access request.

24. What procedures exist in your department for suppression, blocking or correction of personal information?

25. Who authorises these activities?

Data quality

26. Who in your department has responsibility for reviewing personal data for relevance, accuracy and keeping personal data up to date? How often are these activities carried out?

Security

27. Describe in outline the security procedures in operation in your department to keep all information secure. Please describe the physical, logical and technological procedures used.

Destruction or archiving

28. How long is personal information kept in your department before being destroyed or archived?

29. Who authorises destruction?

30. Who authorises archiving?

31. Please describe the archiving procedures in operation in your department.

32. Please give the location of your department's archived information.

33. In what format or on what medium is the archived information stored?

Future Business Requirements

36. Do you foresee in the next twelve months a change in any of the answers you have given? If so, please describe the changes.

GLOSSARY

automatic processing	non-manual 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 data
blocking	prevention of access to data except for legitimate purposes
Commission	the Commission of the European Communities
controller	as defined in the Directive at Article 2 – the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of 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
Council	the Council of the European Communities
criterion of legitimacy	the criteria listed in Article 7 of the Directive that must be satisfied in order that personal data may be processed
data protection notice	a notice to be given to the data subject containing the information required by Article 10 or Article 11 of the Directive as appropriate
data protection officer	an official that may be appointed by the controller, in compliance with national law, to have the responsibilities, inter alia, as listed in Article 18 (2) of the Directive
data subject	as defined in the Directive at Article 2 – an identified or identifiable natural person (see "identifiable person" below)
data subject's consent	as defined in the Directive at Article 2 – 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
data user	a natural or legal person, public authority, agency or any other body which uses personal data for its own purposes
direct marketing	the advertising process by which a company communicates directly with a customer or prospect in order to stimulate an action; usually by mail, telephone, coupon

	advertisement or leaflet
Direct Response Television (or DRTV)	advertising through the medium of television which invites a customer or prospect to respond with an immediate action. For example returning a coupon, phoning for a brochure or ordering a product
encryption	the scrambling of data during transmission to prevent unauthorised access
flag	to put a marker against a record in a computer system in order to differentiate the subsequent treatment
identifiable person	as defined in the Directive at Article é – 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
implementing legislation	national law that gives effect to Community Law
knowledge of the logic	understanding of the criteria and the process by which an automated decision is reached
manual data	data held on paper files
mark	see “flag”
personal data	as defined in the Directive at Article 2 – any information relating to an identified or identifiable natural person (“data subject”)
personal data filing system (filing system)	as defined in the Directive at Article 2 – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis
processing of personal data (processing)	as defined in the Directive at Article 2 – 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
processor	as defined in the Directive at Article 2 – a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller
recipient	as defined in the Directive at Article 2 – 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
register of notifications	the register to be kept of all notifications made to a supervisory authority in accordance with Articles 18 and 19 of the Directive
sensitive data	data of a personal nature such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and concerning health or sex life; referred to as "special categories of data" in the Directive
subject access	the data subject is conferred the right to obtain from the controller certain information relating to the data held and the processing of that data (Article 12 of the Directive)
subsidiarity	the principle by which each Member State has a degree of flexibility and choice in the way in which it implements Community legislation into national law
supervisory authority	the public authority (one or more) within a Member State responsible for monitoring the application within its territory of the provisions adopted pursuant to the Directive
third country	countries other than 15 Member States
third party	as defined in the Directive at Article 2 – 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

III. Data protection and legal persons

1. INTRODUCTION

The aim of this study is to consider to which extend the provisions of the Directive n° 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data may be applicable to legal persons.

The national laws implementing the Directive n° 95/45/EC are very different from one country to another. The objective of the present document is therefore not to make a comparative or exhaustive analysis of the situation of the different Member States, but to present briefly the problematic of the protection of data belonging to legal persons. In case Member States would consider, after having read this document and check their national laws, that legal persons could be concerned by the implementation of the Regulation (EC) n° 2135/98, they would have to answer the questions asked on page 5 under the point 4.

2. GENERALITIES

The Directive was construed with references to the right to respect for private life, the right to freedom of expression (articles 8 and 10 of the European Convention of Human Rights and Fundamental Freedoms and general principles of Community law (fair trial guarantee, effective remedy guarantee, rights to freedom of thought, conscience and religion, the right to freedom of association and the rights not to be discriminated against on such grounds.).

The request to protect the unrestrained and use of personal data of legal persons under article 8 of the European Convention is arguable and ambiguous and the article 10 concerning the freedom of expression can hardly be invoked as a basis for such protection.

Some of the rights protected by the European Convention are inherently limited to "natural persons" such as the right to life (article 2), the right not to be subjected to death penalty, the right not to be subjected to torture, inhuman or degrading treatment or punishment (article 3), the right to liberty and security of person (article 5)…

Private law legal persons are protected by other fundamental rights: rights to protection of their property, right to fair hearing in civil and criminal cases, freedom of association, freedom of expression, rights to be informed of information held on a person by others persons which take significant decisions, right to challenge such data, guarantee of effective remedy against violation of those rights.

Data held on political, religious, trade union or other associations directly affects those fundamental rights.

3. RISKS AND PRACTICAL EFFECTS.

There are a number of distinct areas in which the extension of data protection to the legal persons has a practical effect.

1. **In general.**

The protection of the interests of legal persons in relation to the processing of data on users and subscribers of telecommunications services.

The Directive n° 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector will ensure once fully implemented an equivalent level of protection of fundamental rights and freedoms (in particular the rights of privacy) with respect to the processing or personal data in the telecommunications sector.

There will be no longer any obstacles to the free movement of data on legal persons.

The protection of interests of legal persons in relation to the processing of business information by credit reference agencies, "warning agencies" and the like.

Legal persons are clearly affected by the processing of information on them and some countries already tightly control credit reference and business information.

The application of data protection law to legal persons in one Member State such as Austria, but not in most others, will lead to the imposition of obstacles to data transfers:

- credit reference agencies established in other Member States will have to comply with the Austrian data protection rules when they collect data on Austrian companies, but they are not subject to such rules when they collect data on companies elsewhere.

- disclosure of data on Austrian companies from Austria by third countries parties to such agencies established elsewhere in the Community, will have to conform to the strict rules on data export, contained in the law (disclosures without the knowledge and consent of the companies concerned will be severely limited.).

See point 4 for the question to be answered as far as enforcement is concerned.

The protection of the interests of legal persons in relation to direct marketing.

- Within the direct marketing industry, a distinction is made between "marketing consumers" and "business-to-business marketing". In the majority of Members States, one-person business are entitled to the protection of national law in the respect of the "mailing preference services" which allow people to register the fact that they object to receive direct mail. The ISDN Directive n° 97/66/EC stipulates that Member States must guarantee that the "legitimate interests" of "subscribers other than natural persons" are sufficiently protected in the respect of the sending of unsolicited faxes for advertising purposes.

- Data held by companies on contact persons in other companies is ever-increasing.

These two matters underline the difficulty of distinguishing between "consumers", "businesses", data on other companies and data on contacts within such other companies.

The protection of the interest or religious, philosophical, political or trade union associations and their members affected by the processing of information on such associations.

Collection of data on such association can affect important fundamental rights of both individual and the group, such as the freedom of believe, the freedom to educate one's children in accordance to one's beliefs, the freedom of association and the freedom of association.

Failure to accord a protection under the European Convention on Human Rights creates obstacles to the internal market and also raise questions concerning the compatibility of free data exchanges on such bodies within the EU with the Convention and general principles of Community Law.

2. **In particular.**

The protection of the interests of legal persons in relation to the processing of business information provided by them to State or Community institution for statistical and other purposes.

Companies are enquired to provide ever-increasing detailed information on their financial, environmental and other activities. While the need to provide such information is accepted, concern has been raised about the proper use of such information.

There is a need to apply some protection to the provision of such data notably the principles of purpose-specification and limitation, data security and confidentiality.

These principles can be invoked to the extend that the processing of data is covered by the law of a Member State which does extend data protection to legal persons.

On the other hand, data protection should not be used to shield companies from examination of their environmental, consumer protection or anti-fraud policies. This is basically a matter of balance.

In countries which does extend data protection to legal persons (in Austria, for example), openness can normally ensured under relevant open, flexible clauses : when companies do not have a "protection-worthy interest" in keeping such information secret, restrictive data protection can be left aside.

The protection of the interests of legal persons in relation to the processing of information on them which is used to take decisions which "significantly affect" them (by public and private bodies).

The rationale underlying article 15 of the Directive n° 95/46/CE[5] clearly applies broadly and equally to legal as it does to natural person.

[5] «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, rehability, conduct, etc ;

National public and administrative law often provide specific redress against administrative decisions by public authorities and grant a right of access to data, a right to challenge such data and seek corrections and additions to the relevant files but such law are often inconsistent.

3. The scope of protection to be accorded to one-person business.

One-person businesses, which are natural persons as well as economic actors, enjoy data protection under the Directive n° 95/46/EC. Sole traders can use the rights of access, challenge and rectification, granted to natural persons by this Directive vis-à-vis traders in "business information", credit reference and "warning" agencies and vis-à-vis public authorities.

But the application of various provisions to one-person businesses under the Directive can be mitigated because of the different nature of the interests concerned. Processing of data on a sole trader will, for instance, be more easily justified and access to data can in certain cases be more easily denied if the request comes from a sole trader.

The application of data protection law to "natural persons" only creates an anomaly : if it is right to extend data protection to sole traders, it is not clear why similar protection can not be accorded to corporate businesses.

This situation creates practical matters which have been recognised by Members States to different degrees. For example, Danish law contains some provisions which apply to "consumers" and not to one-person businesses.

Such differences will not immediately affect the principle of free movement of personal data within the internal market because the Directive n° 95/46/EC allows certain divergent practices (article 5) and stipulates that Member States may not invoke such different protection as a reason for restricting or prohibiting the free flow of such data between them (article 12).

The article 30 charges the Working Party to contribute to the uniform application of measures adopted under the Directive and shall inform the Commission if it finds divergences likely to affect the equivalence of protection. The Commission can in such cases make recommendations.

So, the application to one-person businesses of national measures adopted to implement the Directive seems to be an appropriate matter especially if the Working Party gives wider consideration to the application of data protection law to legal persons.

---

2. Subject to the other Articles of the 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 :

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 t put his point of view; or

is authorized by law which also lays down measures to safeguard the data subject's legitimate interests. »

4. **The effect of the new data protection regime in the EU and EEA**.

There will be differences between the laws of Members states as regards the extent to which they accord protection to legal persons, those differences will have a complex effects as a result of certain provisions of the Directive.

In fact, law of all Members States will have an extra-territorial effect resulting from the article 4 of the Directive n° 95/46/CE:

"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 Community."

Even if, of course, the Directive requires this extra-territorial applicability only with regard to the processing of data on "natural persons", the Members States which would apply their law to legal persons would also adopt the extra-territorial approach.

This means that Member States laws that would apply not only to the processing data within the territory of those States, but would also apply to the processing of such data in other countries when the control of the relevant activity is established on the territory of one of these states and that the collection of data on legal person by one of these country would be subject to restrictions while the collection of the same data in another country would not be subject to the same restrictions. This poses obstacles to the internal market.

Concerning transborder data flows, the Austrian law imposes the same conditions as apply to the export of data relating to natural persons from the EU/EEA to third countries (article 25 and 26 of the Directive).

This point also poses obstacles to the internal market but not imposing national restrictions on the processing of data on legal persons in transnational context means that the national protection rules protecting legal persons can be easily evaded by companies established in another EU Member State.

Thus, the diversity of national approaches creates obstacles to the free movement of data on such persons within the Union, especially in a number of context.

4. CONCLUSIONS

Member States shall, as far as the Regulation (EEC) n° 3821/85, as last modified by Regulation (EC) n° 2135/98, is concerned, check :

- whether or not the national laws implementing the Directive n° 95/46/EC in their country extend the data protection rules to the legal persons ;
- whether or not the one-person business are concerned by these same national laws ;
- whether or not the approved workshops are also concerned.

If it is the case :

- which impact these national rules would have for the data concerning the transport companies ;
- which impact these national rules would have for the data concerning the one-person business / one man – one truck companies ;
- which impact these national rules would have for the data concerning the approved workshops ;
- which impact these national rules would have on enforcement and most especially on the possibility to exchange data about companies between enforcement agencies of different Member States.

If there is an impact and as the Regulation (EC) n° 2135/98 is a European legal act, the national laws concerned will have to be modified accordingly.

IV. Data to be accessed and to be used by enforcement officers

The enforcement officers who will be issued a control card will have an unlimited access to the data recorded in the vehicle unit.

They will have also and anyway access to all the data recorded on the driver card, and - via the print-outs and the display - to the very big majority of the data recorded in the vehicle unit.

In order to complete their checks, they can also have to have access to some other information that can be found mainly under a paper format.

Data	**Available in**	**Justifications for having access to these data during roadside checks and company checks**
Name and first name(s) of the driver • Identity of the driver (name, first name(s), social security / national number) • Validity of the DC	VU[6]- DC[7]-PC[8], any other documents	Necessity to know who has committed the infringement for the prosecution
Drivers' activities such as:		
• driving, rest, availability and working times	• VU – DC – PC, Paper disks, print-outs, any other documents	• Necessity to know which infringement have been committed notably against the EU Regulations (EEC) n° 3820 and 3821/85 as last modified
• overspeedings	• VU-PC, Paper disks, print-outs	• Check in some circumstances if the driver has made an overspeeding
• frauds/faults	• VU-DC-PC, print-outs, any other documents	• Necessity to know which infringement has been committed notably against the EU Regulations (EEC) n°

[6] VU = Vehicle Unit (tachograph)
[7] DC = Driver Card
[8] PC = in a PC after the data would have been downloaded from the VU and/or the DC to any PC
[9] As defined in the Regulation (EEC) n° 3821/85 as last modified

		3820 and 3821/85 as last modified
• distances travelled	• VU-DC-PC, print-outs, paper disks, any other documents	• Necessity to cross-check the activities of the drivers
• the journey (from-to)	• VU-DC-PC, print-outs, Paper disks, any other documents as well as GPS data if available	• Necessity to know under which *legis corpus* the driver has performed his activities (AETR or 3820-21/85). Problem also with the extraterritoriality rules and the necessity to know where the infringement has been committed within the EU
• dates	• VU-DC-PC, print-outs, paper disks, any other documents	• Necessity to know when the infringement has been committed to prosecute the responsible person(s)
• time and duration of the activities	• VU-DC-PC, print-outs, paper disks, any other documents	• Necessity to check if the duration is in compliance with the duration laid down in the Regulation (EEC) n° 3820/85 and in the AETR
• status of the activities (single or crew driver)	• VU-DC-PC, print-outs, paper disks, any other documents	• Necessity to check if the duration is in compliance with the duration laid down in the Regulation (EEC) n° 3820/85 and in the AETR as the duration of these activities can change depending on the status of the driver
• VIN-VRN	• VU-DC-PC, print-outs, paper disks, any other documents	• Necessity to identify the vehicle in which the infringement has been committed

• events generated by the drivers	• VU-DC-PC, print-outs	• Part of the drivers activities and as such necessity to check them (see above)
• Technical data	• VU, print-outs	• Necessity to check if the parameters entered into the VU are still valid
• Paper disks	• If available	• Drivers' activities to be checked
• Any relevant document[9]	• If available	• Drivers' activities to be checked
Other information concerning the drivers such as:		
• the salary	• If available	• Cross-check of the driver activities (article 15 of Regulation 3820/85)
• time sheets	• If available	• Cross-check of the drivers' activities
• planning	• If available	• Cross-check of the drivers' activities
• letter of attestation	• If available	• Cross-check of the drivers' activities
• agenda	• If available	• Idem but access limited or even impossible depending on the countries
• bunkering	• If available	• Cross-check of the drivers' activities
• controls (done or on-going)	• VU-DC-PC, print-outs	• *Non bis in indem* rule
• fines	• If available	• *Non bis in indem* rule
Identity of the drivers such as:		
• Date of birth of the driver	• PC, DC, any other document	• Necessity to check the age of the driver

		against the provision of the Regulation (EEC) n° 3820/85 fixing a minimum age to drive some vehicles
• social security/insurance number	• PC, any other document + national network	• See identity of the driver
• family status	• Salary sheets, other company documents	• Not requested
• address	• PC, any other document	• Necessity to know the address of the driver to prosecute him
• Relationship between the driver and the operator and address of the operator	• PC, any other document	• Necessity to check the potential liability of the employer. The level of the fine can be different depending on the relationship between the driver and the operator

V. Data to be accessed and to be used by approved workshops

This table has been produced by the Task Force 3 (TF3) members.

The workshops will have an unlimited access to the data recorded and stored in the vehicle unit.

All these data could be considered by the workshops as indicative, but the TF3 members considered that to check the proper functioning of the digital tachograph, the workshops will have to perform tests. They will not start from the assumption that the fact to have access to some data means that the tachograph records correctly what it is supposed to record and store.

Therefore, except the detailed speed (exception to be confirmed by the TF3 members), the workshops will make no use of the data they will have access to.

Data	**Available in**	**Justifications for having access to these historical data[10]**
Name and first name(s) of the driver	VU[11]- DC[12]-PC[13]	No use
Drivers' activities such as :		
• driving, rest, availability and working times	• VU – DC – PC	• No use
• overspeedings	• VU-PC	• No use
• frauds/faults	• VU-DC-PC	• Necessity to know the malfunctioning of the digital tachograph
• distances travelled	• VU-DC-PC	• No use
• the journey (from-to)	• VU-DC-PC	• No use
• dates	• VU-DC-PC	• No use
• duration of the activities	• VU-DC-PC	• No use
• status of the activities (single or crew driver)	• VU-DC-PC	• No use
• VIN-VRN	• VU-DC-PC	• Check the parameter

[10] The approved workshop could have to have access to all the VU's data in case they would be required to download the VU in conformity with requirement 260 of Annex 1B.
[11] VU = Vehicle Unit (tachograph)
[12] DC = Driver Card
[13] PC = in a PC after the data would have been downloaded from the VU and/or the DC to any PC

		entered into the VU
• events generated by the drivers	• VU-DC-PC	• No use
• detailed speed for the last 24 hours (driven)	• VU	• Check if detailed speed is correctly recorded by the tachograph and for accident purposes if requested by the enforcement officers
• Technical data	• VU	• Check the parameters entered into the VU

VI. Checks to be made by the Member States

Additional checks to be made by the Member States

The data enforcement officers and approved workshops will have access to and could need to use are identified under the points IV and V of this final report.

Therefore, having in mind the explanations given in the parts 2 and 3 of this document, some checks shall be made by the Member States :

1 – The principle of proportionality

Member States shall ensure that enforcement officers and workshops are not going to use means which are not proportional with the objectives they are supposed to reach, according to the Regulation (EEC) n° 3821/85 as last amended.

This check has to be made against the tables presented under the points IV and V of this final report.

2 – Will the data need to be archived ?

If the answer to this question is positive, the Member States will have to answer the following questions :

- What is the justification for archiving these data ?
- Who will have to archive the data ? The enforcement agencies or the Ministry of Justice ?
- For how long ?
- Are they secured ?

3 – Who will have access to these data ?

The different points mentioned below will have to be examined against the provisions of the Directive n° 95/46/EC (see point II of this final report).

- What about the access of these data by your staff ?
- What about the access of these data by other people ?
- What about the access of these data by the persons directly concerned ?
- Is that possible to modify these data ?
- If yes, who can modify these data ?
- What would be the procedure to modify these data ?
- What about the security measures to be taken ?

4 – Will data be transferred ?

If the answer is positive, then the following questions will need to be answered :

- From your country to your country : what about the security measures to be taken ?
- From your country to another EU Member State : what about the security measures to be taken ?
- From your country to a third country : what about the security measures to be taken ?

5 – The extension of the data protection to the legal persons

Member States shall, as far as the Regulation (EEC) n° 3821/85, as last modified by Regulation (EC) n° 2135/98, is concerned, check :

- whether or not the national laws implementing the Directive n° 95/46/EC in their country extend the data protection rules to the legal persons ;
- whether or not the one-person business are concerned by these same national laws ;
- whether or not the approved workshops are also concerned.

If it is the case :

- which impact these national rules would have for the data concerning the transport companies ?
- which impact these national rules would have for the data concerning the one-person business / one man – one truck companies ?
- which impact these national rules would have for the data concerning the approved workshops ?
- which impact these national rules would have on enforcement and most especially on the possibility to exchange data about companies between enforcement agencies of different Member States ?

If there is an impact and as the Regulation (EC) n° 2135/98 is a European legal act, the national laws concerned will have to be modified accordingly.

VII. Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data

Status of implementation of Directive 95/46
on the Protection of Individuals with regard to the Processing of Personal Data

Key to table

- O.J.: Official Journal
- D.P.L: Data Protection Law

Member State	**Status of legislative procedure**	**Next step**
Austria	1) Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 136/2001 of 17.08.1999 that applies to all processing by automatic means. **Original version:** http://www.bka.gv.at/datenschutz/dsg2000d.pdf **English version:** http://www.bka.gv.at/datenschutz/glossd.htm#PDF 2) Entry into force: 01.01.2000. 3) Adopted ordinances: Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999, about countries with adequate DP legislation (Switzerland and Hungary); Verordnung des Bundeskanzlers über das bei der Datenschutz- kommission eingerichtete Datenverarbeitungs register (Datenverarbeitungsregister-Verordnung 2000 - DVRV), Federal Law Gazette II Nr. 520/1999, about the registration procedure; Verordnung des Bundeskanzlers über Standard- und Muster- anwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification. Seven Länder have adopted new DPLs to implement the Directive. These apply to processing otherwise than by automatic means. **Kärnten:** Kärtner Landesdatenschutz-Gesetz (K-LDSG), LGBl. Nr. 59/2000 (Inkrafttreten: 01.01.2000)	

	http://www.bka.gv.at/datenschutz/dsg_ktn.htm **Niederösterreich:** NÖ-Datenschutzgesetz (NÖ DSG), LGBl. 0901-1 (Inkrafttreten: 01.01.2001) http://www.bka.gv.at/datenschutz/dsg_noe.htm **Oberösterreich:** Gesetz vom 1. Juli 1988 über die Auskunftspflicht der Organe des Landes, der Gemeinden, der Gemeindeverbände und der durch Landesgesetz geregelten Selbstverwaltungskörper (oÖ. Auskunftspflicht- und Datenschutzgesetz), LGBl. Nr. 46/1988; idF. LGBl. Nr. 41/2000 http://www.bka.gv.at/datenschutz/dsg_ooe.htm **Salzburg:** Gesetz über die Auskunftspflicht und den Datenschutz, LGBl. Nr. 73/1988, idF LGBl. Nr. 65/2001 (Inkrafttreten 01.07.2001) http://www.bka.gv.at/datenschutz/dsg_sbg.htm **Steiermark:** Gesetz vom 20. März 2001 über den Schutz personenbezogener Daten in nicht automationsgestützt geführten Dateien (Steiermärkisches Datenschutzgesetz-StDSG), LGBl. Nr. 39/2001 (Inkrafttreten: 01.08.2001) http://www.bka.gv.at/datenschutz/dsg_stmk.htm **Vorarlberg:** Vorarlberger Landes-Datenschutzgesetz, LGBl. Nr. 19/2000 (Inkrafttreten: 01.01.2000) http://www.bka.gv.at/datenschutz/dsg_vlbg.htm **Wien:** Wiener Datenschutzgesetz (Wr. DSG), LGBl. Nr. 125/2001 http://www.bka.gv.at/datenschutz/dsg_wien.htm#4	
Belgium	1) Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data 2) modified by the implementation law of December 11, 1998 (O.J. 3.2.1999) English version: http://www.law.kuleuven.ac.be/icri/papers/legislation/privacy/engels/	

	3) Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001. 4) Entry into force: 01.09.2001 (exception for information when the data were not collected from the data subject then three years more).	
Denmark	1) The Act on Processing of Personal Data (Act No. 429) of 31 May 2000 English version: http://www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1 2) Entry into force: 01.07.2000.	
Germany	1) The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May German version : http://www.bfd.bund.de/information/bdsg_hinweis.html English version : The Federal Data Protection Act applies to the federal public sector and the private sector. 2) Entry into force: 23.05.2001. All Länder (except Sachsen and Bremen) adopted new DPLs to implement the Directive. These acts apply to the public sector of the respective "Länder". **Baden-Württemberg:** Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz - LDSG) vom 27. Mai 1991, zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze vom 23. Mai 2000: http://www.baden-wuerttemberg.datenschutz.de/ldsg/ldsg-inh.html **Bayern:** Bayerisches Datenschutzgesetz (BayDSG) vom 23. Juli 1993, zuletzt geändert durch Gesetz zur Änderung des Bayerischen Datenschutzgesetzes vom 25.10.2000 (Inkrafttreten zum 01.01.2001):	

www.datenschutz-bayern.de/recht/baydsg_n.pdf

Berlin :
Berliner Datenschutzgesetz vom 17.Dezember 1990 (GVBl. 1991, S. 16, 54), geändert durch Gesetz vom 3.Juli 1995 (GVBl. 1995, S. 404), zuletzt geändert durch Gesetz vom 30. Juli 2001(GVBl. I, S. 66) (Inkrafttreten zum 5.8.2001) :
http://www.datenschutz-berlin.de/recht/bln/blndsg/blndsg_nichtamt.htm

Brandenburg:
Gesetz zum Schutz personenbezogener Daten im Land Brandenburg
(Brandenburgisches Datenschutzgesetz - bgDSG) in der Fassung der Bekanntmachung vom 9. März 1999
http://www.brandenburg.de/land/lfdbbg/gesetze/bbgdsg.htm

Hamburg :
Hamburger Datenschutzgesetz vom 5. Juli 1999, zuletzt geändert am 18. Juli 2001 (HmbGVBl. S. 216)
http://fhh.hamburg.de/coremedia/generator/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/datenschutzrecht/hamburgisches-datenschutzgesetz-1990-07-05-pdf,property=source.pdf

Hessen:
Hessisches Datenschutzgesetz (HDSG) in der Fassung vom 7. Januar 1999
http://www.hessen.de/hdsb/hdsg98/hdsg98v2.htm

Mecklenburg-Vorpommern:
Landesdatenschutzgesetz vom 28. März 2002 (GVOBl. M-V S. 154)
http://www.lfd.m-v.de/ges_ver/guv/guv_c_20.html

Niedersachsen:
Niedersächsisches Datenschutzgesetz (NDSG) in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22)
http://www.lfd.niedersachsen.de/functions/downloadObject/0,,c299076_s20,00.pdf

Nordrhein-Westfalen:
Gesetz zum schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen-DSG NRW-) idF. der Bekanntmachung vom 9. Juni 2000
http://www.lfd.nrw.de/fachbereich/fach_3_1.html

Rheinland-Pfalz :
Landesgesetz zur Änderung datenschutzrechtlicher

	Vorschriften vom 8. Mai 2002 (GVBl. S. 177) http://www.datenschutz.rlp.de/download/lfdheft1/A1_5_Aenderungsgesetz.htm **Saarland:** Gesetz Nr. 1477 zur Änderung des Saarländischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 22. August 2001 (Abl. S. 2066) http://www.lfd.saarland.de/dschutz/SDSG.htm **Sachsen-Anhalt :** Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) http://www.datenschutz.sachsen-anhalt.de/dsg-lsa/inhalt.htm **Schleswig-Holstein :** Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000 http://www.datenschutzzentrum.de/material/recht/ldsg-neu/ldsg-neu.htm	
Spain	1) Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999). Original version: https://www.agenciaprotecciondatos.org/datd1.htm English version: 2) Entry into force: 14.01.2000.	
France	1) Law 78-17 of 6 January 1978 2) draft implementation law of July 2001 http://www.justice.gouv.fr/actua/loicnild.htm	Discussed in Parliament
Greece	1) Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data Original version http://www.dpa.gr/2472.htm 2) Entry into force: 10.04.1997	
Italy	1) Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996.	Parliamentary discussion about the renew of the

	English version: http://www.dataprotection.org/garante/prewiew/1,1724,448,00.html?sezione=120&LANG=2 2) Entry into force: 08.05.2000 3) Additional legal acts previewed by Act no. 676 of 31.12.1996 (in particular, the Legislative Decrees no. 123 of 09.05.97, no. 255 of 28.07.97, no. 135 of 08.05.98, no. 171 of 13.05.98, no. 389 of 06.11.98, no. 51 of 26.02.99, no. 135 of 11.05.99, no. 281 and no. 282 of 30.07.99 ; the Presidentials decrees No. 501 of 31.03.98, No. 318 of 28.07.99)	delegation to the Government to complete Law 675.
Ireland*	Draft bill submitted to Parliament. Available at www.justice.ie in the section on 'publications' Bill's main provisions available at: http://www.dataprivacy.ie	
Luxembourg	A new DPL has been adopted on 02.08.2002.Entry into force: 01.12.2002.Published in "Mémorial A n° 91 of 13 August 2002 http://www.etat.lu/memorial/memorial/a/2002/a0911308.pdf National Commission for Data Protection http://www.cnpd.lu/	
The Netherlands	1) DPL approved by the Senate on 06.07.2000 (O.J. 302/2000). Original and English version: Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000 2) Entry into force on 1 September 2001. 3) Secondary legislation adopted	
Portugal	1) Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecçao de dados pessoais' English version: http://www.cnpd.pt/Leis/lei_6798en.htm 2) Entry into force: 27.10.1998	
Sweden	1) Directive implemented by SFS 1998:204 of 29.4.98 and	

	regulation SFS 1998:1191 of 03.09.98 English version: http://www.datainspektionen.se/in_english/default.asp?content=/in_english/legislation/data.shtml 2) Entry into force: 24.10.1998.	
Finland	1) The Finnish Personal Data Act (523/1999) was given on 22.4.1999 English version: http://www.tietosuoja.fi/uploads/hopxtvf.HTM 2) Entry into force: 01.06.1999.	
United Kingdom	1) Data Protection Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980029.htm 2) Passed: 16.07.1998 3) Subordinate legislation passed on 17.02.2000. http://www.lcd.gov.uk/foi/foidpunit.htm 4) Entry into force: 01.03. 2000.	

* means that measures have been implementing Commission Decision 95/46/EC have not been notified.

VIII. Conclusion

The problems that could be faced by a Member State, as far as data protection is concerned, could be different from those faced by another Member State, as their implementation of the Directive n° 95/46/EC could well vary on some particular points.

The attention of the Member States shall nevertheless be drawn on the fact that the Regulation (EC) n° 2135/98 supersedes every national law, notably adopted in the field of data protection, and that, consequently, no excuse can be found to not implement this Regulation in case of conflict between this text and national laws on data protection.