EU-MIDT

Implementation Policy Committee

EU-MIDT/IPC/030-2005

Recommendations on Data Management

PREPARED BY: MIDT Secretariat
DATE: 15/12/2005
EU-MIDT IPC – 030-2005

REF : EU-MIDT/IPC/030-2005

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY		MIDT Secretariat (issued by IDT Project on 25/09/2003)	15/12/2005
CHECKED BY	Isabelle DOCHY	Squaris – MIDT Secretariat	15/12/2005
APPROVED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	15/12/2005
ISSUED BY	Secretariat	MIDT	15/12/2005

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

Vägverket

SNRA

Contract n° SUB/B27020B/E1/507.14876/2002

Digital tachograph and data management

Final report

25/09/2003

Per-Arne HOLM (Sweden) : project leader
Hans DRIJER (The Netherlands) : chairman of the Task Force 2
Marie-Christine BONNAMOUR (Cybèle) : general coordinator of the project
Task Force 2 : Author

Executive Summary

In October 2002, the Swedish National Road Administration (SNRA) signed a 30 month contract with the European Commission (reference SUB/B27020B/E1/507.14876/2002) to carry out a project involving all the Member States plus Iceland, Norway and Switzerland.

The purpose of this project is to support the Member States in the introduction of the digital tachograph. The European Commission and the Council of Ministers decided to introduce the digital tachograph in order to:

> *"improve the enforcement of, and compliance with, social legislation relating to road transport, as laid down in Council Regulation (EEC) 3820/85".*[1]

The main aim of this project is to meet that underlying objective. It also aims to ensure that the digital tachograph is introduced in an efficient way and - as far as possible - to harmonise procedures across the Member States.

Under the terms of the contract, reports must be issued on the particular topics listed in the project proposal (reference SNRA/PLE/001). This document has to be considered as the final report on data management.

1. Objective of this report

This report is based on Regulations (EEC) n° 3821/85 as amended by (EC) n° 2135/98 and (EC) 1360/2002 as they stand today.

Regulation (EEC) n° 3821/85 deals mainly with the use of analogue tachographs. It has been amended by Regulation (EC) n° 2135/98, to provide for the introduction of digital tachographs.

The technical specification of the digital tachograph is contained in Annex 1B of Regulation (EEC) n° 3821/85 as amended.

The original Annex 1B was replaced in its entirety by Commission Regulation (EC) n° 1360/2002.

For the purpose of this final report, please note that all references to :

- Regulation (EEC) n° 3821/85 are references to that Regulation as last amended by Regulation (EC) n° 2135/98;
- Annex 1B of Regulation (EEC) n° 3821/85 are references to the version of Annex IB contained in Commission Regulation (EC) n° 1360/2002;
- "provisions" are references to provisions in the Regulation, whereas "requirements" are references to requirements contained in Annex 1B.

[1] Explanatory Memorandum of the European Commission, COM (94) 323 final, page 1

The Regulation (EEC) n° 3821/85 contains a new Article 14.5 on downloading (introduced by Article 1.7.5 of Regulation (EC) n° 2135/98) but it is not clear and complete enough for the Member States to be used at national level.

In other words, Member States will need to regulate at national level to ensure that the data recorded by the vehicle unit (VU) and on the driver card (DC) are available for enforcement purposes.

Therefore, this report looks at how transport undertakings – or more generally anybody using a VU for his/her own account – should manage their data :

- to protect the data from access by unauthorised persons ;
- to avoid losing any data ; and
- to keep the data in a way that allows them to meet the requirements of the enforcement authorities (to be adopted at national level).

This report can also be used by the Member States as the recommendations could easily be turned into national legislation.

2. The main principles and recommendations of this report

The main principles that should govern the management of data from VUs and DCs are that :

- transport undertakings are responsible for their own data ;
- they have to be considered as liable for any loss of data. and
- they must, therefore, be in a position to hand over all data requested by the enforcement authorities within the prescribed time limits.

The conclusions reached by the experts having worked on this topic are that :

- for digital tachographs, there is an obvious need for downloading data for enforcement purposes ;
- downloading is preferred over producing print-outs as printouts will not meet the provisions of Regulation (EC) n° 2135/98 to guarantee the safety and accuracy of the data ;
- downloading should be performed at certain intervals and at certain defined fixed moments ;
- in order to be able to monitor compliance with Regulations (EEC) n° 3820/85, 3821/85 as amended by (EC) n° 2135/98, and (EC) n° 1360/2002, it is necessary to have a continuous record, which can only be achieved by downloading all VUs as well as all DCs of the drivers working under the instructions of a transport company ;
- downloading of DC and VU should be mandatory ;
- there is insufficient legal basis, and no explicit requirement, in Regulation (EEC) n° 3821/85 as amended by Regulation (EC) n° 2135/98 for mandatory downloading of the VU ;

- there is no legal basis at all in Regulation (EEC) n° 3821/85 as amended by (EC) n° 2135/98 for mandatory downloading of the DC.

Therefore, the recommendations are :

- That companies should use the lock-in facility as soon as they begin using a vehicle and lock out immediately before permanently or temporarily transferring control of the vehicle to another company. To ensure the availability of timely data for enforcement purposes, downloading should occur:

- For the Vehicle Unit:

  - ✓ Immediately before permanently or temporarily transferring control of the vehicle to another person[2] or company
  - ✓ If it ceases to function correctly but can still be downloaded
  - ✓ In any case, at least every three months.

- For the Driver Card :

  - ✓ Prior to overwriting of data. The 28-day period referred to in Annex IB of Regulation (EC) N° 2135/98 is dependent on the driving pattern of the driver and also on the memory capacity of the particular card. If, in practice, **all** driver cards have a capacity of at least 32kbytes, we recommend that the driver card be downloaded at least once every 31 days. Otherwise, we recommend that all driver cards be downloaded at least once every 21 days.
  - ✓ Before the driver leaves his/her company (that is, when a driver ceases to be employed by a company or - where companies use self-employed drivers or drivers hired from an agency - at the end of the period for which that driver is used).

- For either/both :

  - ✓ Data will have to be downloaded within 24 hours following a request by an enforcement officer involved in the investigation of a serious incident.
  - ✓ Within 7 days in other cases.
  - ✓ In any case, the downloaded data will be made available to the enforcement officer within 7 days of the request.

- Companies should have a backup system for downloaded data : any downloaded data should be protected against accidental (or other) loss by provision of an adequate backup system.

[2] By this we mean the transfer of a vehicle to a person acting as/or for another **transport operator** not the transfer of the vehicle to a **driver** employed by the same person or company.

Enforcement officers must also require a copy of the original files that have been downloaded to be presented in the original format and with the digital signature intact:

- by VRN and by driver ;
- in the chronological order that they have been downloaded;
  - ✓ with file names to be clearly identifiable.

3. Further information

This report contains more detailed information and analysis which explains the rationale of the recommendations made by the experts.

The issues analysed in this report are the following :

Introduction : How to achieve targets of drivers' hours legislation

Based on the Treaty establishing the European Community and in particular Article 71 (former Article 75) social legislation has been founded and developed to safeguard minimum standards in road transport for

- fair competition
- working conditions
- road safety

As binding guideline to identify the targets, the introduction of Regulation (EEC) n° 3820/85 for both the well known recording device and the new digital tachograph, states :

> *"Community social legislation aims at the harmonisation of conditions of competition between methods of inland transport, especially with regard to the road sector and the improvement of working conditions and road safety;*
>
> *Whereas progress made in these fields must be safeguarded and extended;*
>
> *Whereas, however, it is necessary to make the provisions of the said Regulation more flexible without undermining their objectives;".*

The philosophy behind the content of the existing social legislation must remain at least unchanged. Provisions that are necessary or desirable for the 'old device' are also appropriate for the digital one.

Harmonisation of the social legislation leads to uniform (or at least equivalent) procedures for all Member States. Boundary conditions for the whole field of transport business must be at least comparable in the European Union.

The challenge - good value by using the synergies made possible by free competition - needs firstly a uniform understanding of the EU Regulations which govern the use of digital tachographs. A uniform concept should ensure satisfactory tracking measures that have an impact on the compliance of the daily transport business with the social legislation mentioned above.

1. Main objectives of enforcement

Regulations: uniform and effective controls, efficient controls, less fraud, user benefit

The objectives of the drivers' hours Regulations and the speed limiter Directive are to:

- Ensure fair competition
- Improve working conditions
- Enhance road safety

Effective enforcement is required to ensure that in general the transport companies and drivers will comply with drivers' hours and speed limiter rules.
To ensure fair competition it is essential that enforcement be carried out in a harmonised manner. Directive n° 88/599/EEC prescribes harmonised procedures.

With the introduction of digital tachographs it is important to attain at least the same level of enforcement as with the analogue tachograph. However digital tachographs should also allow more efficient enforcement.

It is also desirable for Member States' enforcement requirements to provide benefits for transport companies and drivers wherever possible, e.g. to assist with fleet management.

A continual objective of enforcement is to minimise the opportunity for fraud and maximise the possibility that fraud will be detected.

2. How to achieve enforcement ?

Data/information. Roadside checks. Company checks. Current requirement to store charts in the company

To carry out any enforcement, it is essential that control officers have access to adequate data relating to the activities of drivers and vehicles.

Checks of drivers' activities should be carried out regularly :

a) at the roadside ('roadside checks') ;
b) at the premises of individual transport undertakings or at the premises of the enforcement officers on the basis of relevant documents and/or data handed over by transport undertakings at the request of the enforcement officers ('company checks').

Checks of vehicles should include:

a) Calibration of vehicle according to the Regulation (EEC) n° 3821/85 ;
b) Operation of speed limiter, in compliance with Directives n° 92/6/EEC, 2001/11 and 2003/26.

2.1 : Roadside Check

According to Articles 2 and 3 of Directive n° 88/599/EEC, Member States shall carry out roadside checks to ensure compliance with Regulation (EEC) n° 3820/85.

Comparison of the current and the future situations:

Analogue tachograph	Digital tachograph
Charts for the current week and the last day of the previous week Conclusion Data are accessible If no chart used then no data available except from secondary sources	VU and DC data are accessible through printout, display, retained print-outs and data downloaded (downloading is only possible if the enforcer has the appropriate equipment) Conclusion Data are accessible If no DC used then data still available from the VU, though these data will not be allocated to a driver Vehicle is present, therefore vehicle and speed limiter parameters can be checked.
Conclusion: Data are not accessible	Conclusion: Stored data are accessible but will require further enquiries to establish the driver's identity

From the above comparison it can be seen that, for a roadside check, data from driver cards will be accessible to much the same extent as data are currently accessible from charts.

In the case of the digital tachograph, data are also accessible from the VU.

Sub-conclusion :

With the analogue tachograph, data from charts are accessible during a roadside check. With a digital tachograph, data from the DC are accessible to almost the same extent as data from charts. In addition, data are also available from the VU. Where a driver chooses not to use a chart/DC, then data from a VU will still be accessible, but will not be allocated to a specific driver. Moreover, driving without a chart is always an offence. Driving without a card is not an offence in some circumstances and will therefore be more difficult to control.

It has also to be clear that in a case where a driver, has driven another vehicle earlier in that day or week, the data recorded in the VU of that previous vehicle will not be accessible to the enforcement officer, who might then not be aware of work that driver had performed without his driver card.

2.2. : Company Check

According to Articles 2 and 4 of Directive n° 88/599/EEC, Member States should carry out company checks to ensure compliance with Regulation (EEC) n° 3820/85.

Comparison of the current and the future situations:

Analogue tachograph	Digital tachograph
Data available Charts stored in company for the last year If no chart used then no data available except for secondary sources.	Data available No equivalent requirement for storage of data at the company premises. DC is with the driver and not in the company, therefore data are not accessible. VU's data are in the vehicles and therefore not in the companies. If the period under investigation is more than the duration of the contents of the DC, then full data will not be available - indeed, will no longer exist. Although there may be print-outs available, there is no legal requirement to store them in a particular place. The same applies to downloaded data .

Conclusion – Analogue Tachograph: Data are accessible

Conclusion – Digital Tachograph: In general data are not accessible

Note: some vehicles and drivers may never come to the company premises.

Driver-related data will only be stored in the VU of the vehicle being driven at that time and in the driver's DC if inserted.

Sub-conclusions:

From the above comparison it can be seen that, for a company check, data from charts will generally be accessible in the company. As there is currently no explicit obligation to store data from digital tachographs in the company, then data from DCs and VUs will generally not be accessible in the company.

Where drivers do not use DCs, data will still be available in VUs but it will not be allocated to a particular driver.

Data from digital tachographs will only be accessible if the company chooses voluntarily to keep a complete set of print outs or downloaded data from each DC/VU accessible in the company premises or at another location agreed by enforcement authorities.

3. Legal requirements

recording, storage, availability, responsibility for compliance

3.1. : Introduction

Downloading of data is a technical facility described in the Regulation (EC) n° 2135/98. It was defined to allow both operators using their company card and enforcers using their control card to download the data recorded for their own purpose - operators mainly for freight and fleet management, and enforcers for analysing drivers' activities with the help of software. Downloading of data can also be performed by approved workshops using their workshop card.

The Council when formulating the Regulation in 1998 considered that downloading should remain a national competence:

- each Member State being responsible for organising enforcement of Council Regulation (EEC) n° 3820/85 in its own country;
- each Member State defining the operations they have to perform;
- operators having the freedom, in an open market, to choose to use, or not use, the downloading facility for their own purposes.

3.2. : Comparison of requirements for charts and digital records

Article 14 paragraph 2 of Regulation (EEC) n° 3821/85 states:

> *"The undertaking shall keep the record sheets in good order for at least a year after their use and shall give copies to the drivers concerned who request them.*
>
> *The sheets shall be produced or handed over at the request of any authorized inspecting officer."*

The acceptable delay for collection of charts is not defined.

Relating to digital tachographs, Article 14 paragraph 5 of Regulation (EEC) n° 3821/85 (2135/98 Art. 1, paragraph 7, sub 5) states:

> *"Member States shall ensure that data needed to monitor compliance with Regulation (EEC) No 3820/85 and Council Directive 92/6/EEC of 10 February 1992 on the installation and use of speed limitation devices for certain categories of motor vehicles in the Community which are recorded and stored by recording equipment [read: VU] in conformity with Annex 1B to this Regulation can be made available for at least 365 days after the date of their recording and that they can be made available under conditions that guarantee the security and accuracy of the data. Member States shall take any measures to ensure that the resale or decommissioning of recording equipment cannot detract, in particular, from the satisfactory application of this paragraph.*

Sub-conclusion :

There is a mismatch between the requirements for analogue and digital tachographs. For analogue tachographs the requirement to maintain and hand over record sheets is explicitly defined. For digital tachographs the detailed requirements are left to Member States to specify.

Member States therefore have a legal responsibility to ensure compliance with the following points a) to d) :

a) availability of data needed to monitor compliance with (EEC) Regulations n° 3820/85 and 3821/85 (determined by Article 15 of Regulation (EEC) n° 3820/85);
b) availability of data for at least 365 days after they were recorded in the VU;
c) availability of data under conditions which guarantee security and accuracy;
d) continued availability of data even if the vehicle and the VU have been sold or decommissioned.

Points a), b) and d) could be achieved by maintaining a complete set of print-outs (with signatures) from all VUs of that company's vehicles, or by maintaining a complete set of downloaded data (with digital signatures) from those VUs. Both methods have equal legal value.

Considering c), downloaded data with digital signature will achieve the required security and accuracy; printouts are only pieces of paper which are easy to fake.

Sub-conclusion:

Therefore, although printouts would appear to meet the requirements of this paragraph, only downloading of the VU will fully meet the requirements. It should be noted that there is no explicit or implicit requirement for downloading of DCs.

Downloading has the additional benefits:

- Making data more 'available'
- Providing a back-up of data in the event of failure of VU/DC (normal good practice)

3.3. : Responsibility for compliance

The employer is responsible for his employees.

In the case of hired drivers, the general tendency - based on national systems - is to place the responsibility on the transport undertaking under whose control the driver of the vehicle performs his duties, to the exclusion of the employer which merely supplies labour (Ref. ECJ Case: Auditeur du travail vs Bernard Dufour, Crey's Interim, Case 76/77).

See Appendix B for a further explanation.

Sub-conclusion :

The employer is responsible for his employees. In the case of hired drivers, responsibility rests with the company under whose control the driver operates.

4. Data Available and required for enforcement

charts, VU, driver card, needs of enforcement, comparison current - future situation

Availability of data is discussed further in Appendix C, including how availability of data is influenced by downloading.

4.1. : Available on Charts

Storage of one day on each chart, and with charts stored in the company for 1 year:

- Driving, and rest times for one particular driver; some information relating to availability and working times
- Detailed speed for each day
- Vehicles driven each day entered by driver
- Detailed start and end location for each journey entered by driver
- Odometer (km) entered by driver at the beginning and end of journey
- Detailed distance trace
- Manual entries on rear of chart (e.g driver activities when away from a vehicle) entered by driver.

- Marks representing events such as opening/closing of the tachograph (insertion/removal of charts/loss of power supply).

4.2. : Available in VUs

Storage of approximately 365 days of data:

- Driving times of different drivers of that vehicle, along with periods of rest, availability and other work if recorded using the switch provided on the vehicle.
- Driving without card
- Speed (for the last 24h of driving)
- Overspeeding events
- Other events, e.g. loss of power supply
- Time adjustments
- Odometer (km) for beginning and end of journey entered automatically
- Manual input data which only consist of a symbol which indicates that out of scope work has been undertaken or that rest has been interrupted by movement on or off a ferry boat or train ;
- A flag indicating whether, at card insertion, the driver has manually entered or not activities on his driver card ;
- Country/region for start and end of journeys

4.3. : Available in DCs

Storage capacity of approximately 28 days (see requirement 200 of Annex 1 B) :

- Only driving periods will be recorded automatically on the DC ;
- information relating to rest, availability and working times will require an active intervention from the driver ;
- when away from a vehicle, drivers are not obliged to enter manually their activities on their DC despite the technical facilities exist ;
- Vehicles driven which may belong to different companies ;
- Country/region for start and end of journeys ;
- Odometer/km for times of insertion and withdrawal of DC ;
- Some events, faults and control data.

4.4.: Needs for enforcement

For enforcement of Directive n° 92/6/EEC there is the need for details of vehicles driven, detailed speed, overspeeding events. These data can be found on charts and in VUs.

For enforcement of Regulation (EEC) n° 3820/85 there is the need for data related to the driver – driving and rest times and for Regulation (EEC) n° 3821/85 the need for vehicle data (calibration, etc…) and driver data.

The provisions of the Directive n° 95/46/EC on data protection also apply to enforcement activities. Therefore only data necessary for enforcement activities may be used.

4.5. : Comparison of the analogue tachograph with the digital one

See Appendix C for a more extensive comparison of availability of data from analogue and digital tachographs.

Sub-conclusions:

Detailed speed and distance information is permanently recorded on charts. Digital records of detailed speed are overwritten after 24h of driving. Therefore tracing of journey details may only be possible for the period over which these data are retained.

Some data are only in the DC (e.g. any manual entries made voluntarily of activities performed when away from a vehicle). Some data are only in the VU (e.g. driving without a card, speed and overspeeding information). Data relating to an individual driver who has driven several vehicles will be spread over several VUs, possibly belonging to different companies.

Therefore, in order to check compliance with Regulations, data must be available from both from VUs and DCs.

For a roadside check the required data are accessible as the relevant DC and VU are there at the time (except where a driver has been driving without a card, in which case only data in the VU of the vehicle being checked will be available). For a company check the control officer only has access to data accessible at the company premises. Therefore information from the relevant DCs and VUs must be made accessible at the company premises. To check compliance of a specific driver, data from VUs alone are not sufficient – data are also required from DCs.

5. Action required by introduction of the digital tachograph

comparison charts - VU/DC, need for downloading?

How are data available without downloading as it stands now?

- driver related data on DC for the last +/- 28 days ;
- vehicle related data on the VU for the last +/- 365 days ;
- some driver related data on all /spread VUs for the last +/- 365 days ;
- some vehicle related data spread amongst the DCs of all the drivers the last +/- 28 days ;
- driving without DC is only in the VU as 'driver unknown'.

To maintain all the data available related to individual drivers, the contents of all VUs must be maintained for 365 days.

To identify all the data related to particular drivers that are only stored in VUs, the contents of all the relevant VUs must be collected together and appropriate data must be extracted. It is impractical to do this other than by downloading.

Sub-conclusion:

Not all data related to drivers are stored in VUs – some are only stored in DCs (see section 4.3), and these data may only available for +/- 28 days. If those data are also to be maintained for 365 days then DC contents must be either printed out or downloaded. To guarantee the required accuracy and security then downloading of DCs is the only viable option.

6. Explanation of Downloading

description, remote downloading, security mechanisms, data protection implications, downloading and digital signatures

6.1. : Description

According to Annex 1B (Requirement 010), downloading (via the front panel connector) is not possible in the operational mode. However according to requirement 011, the recording equipment (VU) can in operational mode (with certain restrictions) output data to external interfaces.

Downloading can be carried out by connecting an Intelligent Dedicated Equipment (IDE) to the calibration/downloading connector on the front of a VU. The IDE might be a PC, a laptop or other similar computer or might be a dedicated unit.

An appropriate card (Control, Company or Workshop) would then be inserted into the front of the VU, thus setting the VU into the appropriate mode of operation. Data would then be copied with the digital signature from the VU via the IDE to an external storage medium (ESM). In practice the ESM may be part of the IDE.

Both the VU and DC can be downloaded. If a DC is downloaded, it must be done in its entirety. It is not possible to download only particular days.

Downloading of the VU can be performed by selecting one or more defined days (a day = a calendar day).

A DC can be downloaded simply by inserting the DC into a card reader attached to an IDE. No other card is needed to activate the downloading.

There are no European harmonized standards for the software to run the IDE.

6.2. : Remote Downloading

Remote downloading is different from normal downloading in that:

- the IDE is generally at some distance from the VU/DC being downloaded. The link between VU and IDE is indeterminate and may involve radio, GSM, internet or whatever ;
- the appropriate card need not be inserted into the front of the VU. Authentication can instead be carried out between a company card and the VU via the remote link [remote downloading of the VU is only possible using a company card].

As no authentication is needed to be able to download DCs, there is nothing to restrict remote downloading of DCs.

The primary constraints on remote downloading are:

- to achieve company mode authentication equivalent to inserting a company card into the front of the VU ;
- to protect the data passing between VU and IDE over the remote link in case the data are also received by a non-authorised body.

The mechanism to be used for protection of data passing between VU and IDE is not defined in Annex 1B.

6.3. : Security mechanisms

For enforcement purposes it is of vital importance that data made available can be recognized as genuine data. For this purpose a digital signature is added to the downloaded data; i.e. one digital signature for all the data on the DC and one digital signature for each day downloaded from the VU.

From the perspective of security of the downloaded data, the medium through which the data will be downloaded does not make any difference. The data may be downloaded using GSM or wire or by

some other means. Of course, the medium in itself might not be secure. But from the viewpoint of those enforcing the drivers' hours rules, what matters is whether the data are genuine.

The security objectives relating to downloaded data are :

- to ensure that it is possible to tell whether downloaded data have been changed after they have been downloaded ;
- to be able to prove that the data came from the VU/card as claimed.

To achieve these objectives, the data are protected by the addition of digital signatures. A signature is generated by compressing the data to a manageable size, and then encrypting the result. The signature is then added to the end of the data and stored with the data. If the data are altered, the digital signature will no longer match the data.

It is important to note that privacy of the data is not considered a security issue, and therefore the data themselves are not hidden by encryption.

See Appendix D.

6.4. : Data protection implications

Downloading of data, in the framework of the Regulation (EEC) n° 3821/85 as last amended by Regulation (EC) n° 2135/98 leads to some questions regarding the rules established on one side by the Directive n° 95/46/EC on the protection of individuals with regards to processing of personal data and of the free movement of such data, and on the other side by the Directive n° 99/93/EC on a Community framework for electronic signatures.

These provisions are wide enough to embrace downloading wherever the data are stored, in EU Member States, in the companies, in their sister companies, kept by ad hoc service providers etc…

Member States can use national rules to define the ways in which data must be stored and presented to control officers during company checks.

Nevertheless, Article 6 of Directive n° 95/46/EC, states that data must be:

- *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ;*
- *adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed ;*
- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.*

Article 7 of Directive n° 95/46/EC states that data may be processed only if:

- *it is necessary for compliance with a legal obligation to which the controller is subject*
- *it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.*

When more than 20 separate lock-in/lock-outs have occurred, then earlier data will no longer be locked to a specific company. Other companies will be able to download this previously locked data, which will include data which are 'personal data' for the purposes of the data protection provisions. Access to such data should be restricted. However, requirement 011 states that, in company mode, access to data is free provided that the data in question are not locked by another company. Therefore data older than the last 20 lock-in/lock-outs will be available to anyone with a company card.

Sub-conclusions :

Driver-related data are considered as personal data according to Directive n° 95/46/EC.

Enforcement officers must not ask for, collect, or store, more data than needed to verify compliance with the rules on driving, resting, working and availability periods.

Due to the fact that a DC may only be downloaded in its entirety, enforcement officers will get access to more data than they may legitimately use. During a roadside check there may be access to 28 days or more of activities. Directive n° 88/599/EEC only requires enforcement officers to check the last 8 to 12 days of activities.

Directive n° 95/46/EC requires controllers/enforcement officers to restrict themselves according to the principle of proportionality. Therefore the facilities provided by the driver cards for downloading may make it difficult for enforcement officers to respect the requirements of the Directive n° 95/46/EC.

The requirement according to Directive n° 88/599/EEC to check 8 to 12 days is unclear – is this a maximum or a minimum requirement ? There are differences of interpretation.

Any companies that do download and store data must be registered under data protection legislation.

To comply with data protection requirements it may be advisable to encrypt data stored in an ESM, or otherwise restrict access by unauthorised persons (for example, by requiring a password in order to access the data).

Further information can be found in Appendix E.

6.5. : Downloading and Digital Signatures

Directive n° 1999/93/EC imposes on Member States the obligation to ensure that an electronic (digital) signature is not denied legal effectiveness and admissibility as evidence in legal proceedings.

See Appendix E.

6.6. : Downloading of VUs in short-term hired vehicles

Which company should lock-in the driving etc… records in the VU of a hired vehicle ?

- No lock-in would mean that data in the VU would not be attributed to any particular company.
- A lock-in by the hiring company would allocate the activities correctly. This may not be possible if the hire takes place away from the hiring company's premises. If downloading is not carried out reliably at the end of each hire period then there may be significant difficulties in getting downloaded data later. Downloading to the company could be difficult in the case of hire/use of a vehicle away from the company. The 20 lock-in/lock-out cycles would pass quickly, leading to data becoming available to unauthorised persons.
- A lock-in by the company supplying the hire vehicle would have certain advantages. Only the hire company would have access to data from downloading, but that company would have access to all data. The hire company would then be responsible for providing the downloaded data to the hiring company. It would be far less likely that 20 lock-in/out cycles would pass before locked data had been overwritten, helping to protect the data from unauthorised persons. The company hiring out vehicles may not be within the scope of these Regulations.

Sub-conclusion :

Lock-in/lock-out and downloading of hire vehicles and allocation of data to the correct company is a problem in need of a solution.

It is proposed to encourage the users of the vehicles to use the lock-in / lock-out facilities correctly:

- to ensure that the relevant data will always be downloadable ;
- to ensure that companies prevent unauthorised persons from accessing their drivers personal data

7. Reasons for Downloading

data available at a central point, maintain continuous records, timely data, avoid loss of data, recognising incidents, DL from VU, DL from driver card, DL from workshop card

7.1 : Data available at company premises

Without a central store for data the enforcement task becomes almost impossible. To collect sufficient data to establish whether a particular company was obeying the rules would require the control officer to deal with potentially many sites and/or vehicles which may be difficult to locate.

Central storage is also convenient for the transport company as it will allow it to monitor compliance with the drivers' hours in accordance with Regulation (EEC) n° 3820/85 and Directive n° 92/6/EEC on installation and use of speed limiters.

Currently charts are stored in one place in the company premises. This practice seems to be common and not based on any explicit European or national legal obligation. To maintain this arrangement, data from digital tachographs should also be stored centrally.

If a transport undertaking operates from several sites or hires drivers not employed by that undertaking, then who is responsible to ensure that drivers respect the requirements of Regulations (EEC) n° 3820/85 and 3821/85? Despite the fact that the responsible body is not specified in these Regulations, the European Court of Justice has decided that transport undertaking under whose control the driver of the vehicle performs his duties - to the exclusion of the employer which merely supplies labour - is responsible in these circumstances (Ref. ECJ Case: Auditeur du travail vs Bernard Dufour, Crey's Interim, Case 76/77).

In the absence of any provision determining the localisation of the responsible transport company, the national laws of the Member States are applicable, and these can differ from Member State to Member State.

See Appendix F.

This leaves different solutions in different Member States. In some it is the place where disposition is done, and in others it is the place of the head office of the transport undertaking.

These different legal concepts can lead to situations where no Member State has the authority to check drivers hours.

Sub-conclusion :

There is a need to identify for each transport undertaking a competent body responsible for ensuring compliance with the regulations. Currently the way of identifying this competent body varies between Member States such that some undertakings are not covered. There is therefore a need for a European harmonised legal concept covering the authority for checking compliance with drivers' hours regulations.

7.2 : Maintain complete records

For enforcement purposes it is of vital importance to maintain a complete record of driver and vehicle activities after the VU/card memory has been filled and old data are being overwritten ('complete data' is defined in Appendix A).

7.3 : Maintain records in the case of prosecution

In the case that a driver is prosecuted for a drivers' hours offence, the driver involved is likely to want to defend himself in court. He will need to be able to provide evidence supporting his defense.

Where the relevant data are stored in one or more VUs he will be able to download the relevant data and present it in court. However some data are only available on the DC. Any data stored on a DC are overwritten within a certain number of days.

As indicated in the following paragraph, prosecution for drivers' hours offences may be six months after the event and in some cases/Member States up to 5 years later. Within these timescales any data on a given driver's DC will have been overwritten, probably many times. Unless data have been downloaded and stored appropriately, drivers will not have access to the data required to defend themselves in court.

7.4 : Timely data

To ensure the timely availability of data to enforcement officers all downloading must take place before those data become too old for prosecution purposes (and allow a reasonable period in which enforcers can inspect those data). This may vary from one Member State to another.

The important factor is the age of the infringement being used for the prosecution. The data downloading will take place some time after the infringement, and the data must still be available in sufficient time.

Austria	The statutory period for infringements is 6 months.
Belgium	The statutory period for infringements depends on whether it is a "délit" or a "contravention". The period is 6 months for the minor offences. The period is generally 5 years for serious offences, period which could be reduced to 1 year in some circumstances.
Denmark	The statutory period for infringements is 1 year.
Finland	The statutory period for infringements is 2 years.
France	The statutory period regarding infringements depends on whether it is a "délit" or a "contravention". In case of a "contravention" the period is 1 year, otherwise it is 3 years.
Germany	The statutory period for infringements varies from 6 months (minor) to 2 years (severe).
Greece	/
Ireland	The statutory period for infringements is 2 years.
Italy	The statutory period for infringements is 5 years, starting from the date when the infringement has been committed.
Luxemburg	Infringements on driving and rest times are considered as misdemeanours ("délits"). The statutory period is 3 years.
Norway	The statutory period for infringements is 2 years.
Portugal	The statutory period for infringement is 1 year from the date of the infringement when the fine does not exceed 750 000 PTE (approx. 3.750 Euro). The statutory period for infringement is two years from the date of the infringement, when the fine exceeds this amount.
Spain	The statutory period for infringements varies from 1 year (minor) to 3 years (severe).
Sweden	The statutory period for infringements is 1 year.
The Netherlands	The statutory period for infringements is 2 years.
UK	The statutory period for infringements is 6 months. For serious fraud offences there is no limit.

In the case of prosecutions taking place in more than one Member State, each Member State will collect data in accordance with local requirements. The collected data may then need to be transferred between Member States. There is a risk that data collected in time to meet the requirements of one Member State may be unusable by another Member State as, for them, they will be out-of-date.

Sub-conclusion :

There would be benefit in harmonising the time allowed for collection of data for prosecutions. Given that this level of harmonisation is unlikely in any reasonable time period, there is a need to instead harmonise the period in which companies must collect data (not necessarily restricted to downloaded data).

The time allowed for collection should accommodate the most stringent Member State requirement.

7.5 : Avoid loss of data

Risk analysis. When data can no longer be made available?

Following the requirements of Regulation (EEC) n° 3821/85 (Art. 14 paragraph 5), Member States are required ensure that operators to maintain records for at least 365 days.

However, operators may fail to maintain records for at least 365 days due to equipment failure or (for instance) fraud attempts.

Comparing the current situation with the future, a chart contains only one day of data; the DC contains +/-28 days and the VU contains +/-365 days. Therefore the effect of loss or failure of a DC or VU is much greater than that of the loss of a chart. Accordingly, more care should be taken to guard against data loss.

Examples	Backup	How much data might be lost
Breakdown VU	part. On DC or DL or print-out	+/- 365 days
Breakdown DC	part. On DC or DL or print-out	+/- 28 days
Loss of power to VU	part. On DC or DL or print-out	old data not lost, but no new data recorded
Disposal of VU	part. On DC or DL or print-out	+/- 365 days lost
Loss of DC	part. On DC or DL or print-out	+/- 28 days
Technical inability of DL	Data to be downloaded will remain on DC/VU but some or all of the data may be overwritten before successful downloading takes place. Some data may also be available from print-outs.	any data overwritten before successful downloading takes place
Overwriting (mainly DC)	part. On DC or DL or print-out	anything older than +/-28 days
Loss of downloaded data	Part in the VU and on DC and back-up of these downloaded data	All potentially if no back-up of the downloaded data was made

In the case of downloaded data, the original data may no longer be available (e.g DC data have been overwritten). Therefore a sensible backup must be maintained of downloaded data.

This is not a special requirement for downloaded data as such, only normal good practice.

Sub-conclusions :

The only way to avoid loss of data in the event of equipment failure is to have those data stored (backed-up) outside that equipment. In the case of VU and DC, this can be achieved either by downloading or by taking and storing printouts. However, print-outs will not provide the required security (see section 3.2).

In the case of downloaded data, a back-up of these data should be made as an additional safeguard against loss of the downloaded data.

In the absence of an effective backup, the loss of data may be substantial.

7.6 : Ways of recognising incidents of missing data from the point of view of enforcers

Looking at the list in the paragraph above, each of the incidents will lead to the loss of data. The enforcers' need is to identify these gaps and to fill them using data from other sources:

- breakdown of VU or DC can be recognised at the time of an inspection ;
- loss of power to VU will be recorded as fault in VU and in the DC ;
- disposal of VU will be identifiable by the date of the installation of the new VU recorded in the VU, and perhaps by lack of data older than a certain date ;
- compare current data with data previously downloaded relating to this vehicle to ensure continuity ;
- if there is no downloading/print-outs and the ownership of the vehicle is older than the installation data of the VU, then there are gaps;
- companies may try to 'lose' data by various means, one of which could involve replacement of the VU and falsifying the certificate of undownloadability[3] ;
- theft of a DC – Article 16 (3) requires a formal report in the MS where theft has occurred; it should be possible to confirm that a theft has been reported by checking national data base/Tachonet ;
- loss of a DC – Article 16 (3) requires a formal report to the MS which issued the card; it should be possible to confirm that a theft has been reported by checking national data base/Tachonet ;
- damage or malfunction of a DC – Article 16 (3) requires the card in question to be returned to the issuing authority of the Member State where he has his place of normal residence; again, details should be on national data base/Tachonet ;
- failure to successfully download a VU - previously downloaded data may be available up to a certain date; in addition the data which have not yet been downloaded may still be in the VU (which will normally keep data for at least one year). If the VU itself has failed then downloading may not be possible, in which case the operator should have a certificate of undownloadability[4] ;
- failure to successfully download a DC - previously downloaded data may be available up to a certain date; in addition, the data which have not yet been downloaded may still be in the DC, but old data may be lost (a card will normally retain data for at least 28 days, and a card with a large memory capacity may keep data for several months).

[3] See requirements 260 and 261 of Annex 1B
[4] See requirements 260 and 261 of Annex 1B

7.7 : Data not available from VU

VU's data are vehicle related.

Manual entry data, made voluntarily, are only stored on the DC and can therefore only be obtained by downloading it.

When driving without a driver card, the identity of the driver is missing.

7.8 : Data not available from DC

DC's data are card holder related.

DCs will not contain any record of driving without a card. It will be necessary to download VUs in order to establish whether driving without a card has taken place.

Driver cards will not contain detailed speed data, nor records of overspeeding.

7.9 : Workshop Cards

Nothing in the Regulations requires the data stored on workshop cards to be downloaded.

However, Member States rules generally require records. It is considered good practice.

7.10 : When to Download

The objective of downloading is to ensure the availability of timely data for enforcement purposes. Downloading should therefore occur as follows.

- For the Vehicle Unit:

  - ✓ Immediately before permanently or temporarily transferring control of the vehicle to another person[5] or company
  - ✓ If it ceases to function correctly but can still be downloaded
  - ✓ In any case, at least every three months

[5] By this we mean the transfer of a vehicle to a person acting as/or for another **transport operator** not the transfer of the vehicle to a **driver** employed by the same person or company.

- For the Driver Card :

  - ✓ Prior to overwriting of data. The 28-day period is dependent on the driving pattern of the driver and also on the memory capacity of the particular card. If, in practice, **all** driver cards have a capacity of at least 32kbytes, we recommend that the driver card be downloaded at least once every 31 days. Otherwise, we recommend that all driver cards be downloaded at least once every 21 days
  - ✓ Before the driver leaves his/her company (that is, when a driver ceases to be employed by a company or - where companies use self-employed drivers or drivers hired from an agency - at the end of the period for which that driver is used).

- For either/both :

  - ✓ Data will have to be downloaded within 24 hours following a request by an enforcement officer involved in the investigation of a serious incident. Within 7 days in other cases.
  - ✓ In any case, the downloaded data will be made available to the enforcement officer within 7 days of the request.

Sub-conclusion :

Downloading of VU and DC should be undertaken at certain defined fixed moments as well as at regular intervals.

8. Storage and retrieval of downloaded data

data storage requirements, providing data to enforcers, benefits

8.1. : The Real Data Storage Requirements

Data must be stored reliably such that what is later recovered is exactly what was stored. Records must be complete so that a complete history is available.

The stored data must be made available to control officers in a form in which they can use them and at a convenient location .

Stored data files must be sufficiently identified such that it is possible to satisfy requests for data relating to specific drivers/vehicles and specific dates.

The data must be made available at the time when they are needed.

For further details see Appendix G.

8.2. : Where to store downloaded data

The current Regulations require the transport undertaking to store and make available data (charts). Although the place for storage is not mentioned in the Regulations, it is common practice in all Member States that charts must be stored in the company premises.

Considering this common practice, unless alternative arrangements have been explicitly defined, Member States should also require storage of the data from the digital tachograph at the company premises or at any other convenient place by prior agreement with the enforcement authorities.

Sub-conclusion :

Data from analogue tachographs must be stored in the company premises.

In addition, the transport undertaking may be required, at the request of a competent inspecting officer, to hand over stored charts. In the case of stored digital data the company should, on request, be required to hand over a copy of the stored digital data.

To achieve the enforcement objectives relating to accessibility of data, data from DCs and VUs should be downloaded by (or on behalf of) the transport undertaking on a regular basis and stored such that the data are provided immediately from the company premises or at any place convenient for the enforcement officers. This does not necessarily require physical data storage in the transport company.

Sub-conclusion :

Data from digital tachographs (from VUs *and* DCs) must be immediately provided, either from the company premises or at any place convenient for the enforcement officers.

8.3. : Proposal for common way of presenting data to an Enforcement Officer

Data must be provided upon demand on storage media specified by the enforcement authorities and must include the data in the format specified in Annex 1 B complete with the digital signature.

Enforcement officers should also have the ability to require the data to be presented :

- sorted by VRN or by driver ;
- in chronological order.

One way to achieve this might be to use clearly identifiable file names such as :

DownloadedData<VehicleIdentification or card number><DateOfDownloading>
<DownloadedDataStartDate><DownloadedDataEndDate>

Then without reading the file you could identify that the file contained:

- Downloaded Data
- from a particular vehicle or from a particular driver card
- which was downloaded on a particular date, and
- the period of activity covered by that file

8.4. : Benefits of the proposal

There are numerous benefits:

- the means and details of data storage become unimportant. Any convenient storage medium may be used including any to be identified in the future.
- The location of the storage place for downloaded data becomes unimportant. Data may be stored remotely if appropriate, so long as access to the data is available at the company premises or alternatively at a point specified by the enforcement officer.
- The means of access to the data is exactly as already needed by control officers.
- The downloaded data will be archived and accessible to the enforcement officers almost in the same way charts are accessible today.

9. How to transfer data for storage purposes

According to the conclusions of Chapter 8, charts must be stored centrally in the company premises. Digital data need only to be downloaded and made immediately accessible from the company premises or at any convenient location to be specified by enforcement officers.

A comparison of today's and tomorrow's situation will show how these Regulations can be met by the transport company which is legally responsible for providing the requested data.

9.1. : Introduction

The location of the vehicle or DC during downloading is unimportant provided that the data downloaded are subsequently stored and made accessible from the company premises or at any convenient location to be specified by enforcement officers.

Alternative methods of downloading are (non exhaustive list):

i) make print-outs and send them by mail (though this would not provide the desired degree of security – see section 3.2),

ii) to download data locally or alternatively at a workshop and send a copy of the downloaded data to the company premises (e.g. on a floppy disk) or

iii) download remotely.

9.2. : Consequences due to lock-in/lock-out

The Regulation does not require the company to lock-in its data.

If a company chooses not to lock-in using its company card then data would not be allocated to the company using the vehicle and indeed may be allocated to the company which previously used this vehicle.. Therefore, any subsequent company can download data relating to the first company (which are not locked). It must be assumed that, by not locking-in, the first company has given silent consent to subsequent companies having access to their data.

Requirement 150 of Annex 1B requires that Company mode access rights be satisfied for remote downloading. Therefore remote downloading can only be carried out using a company card.

See Appendix H for further details.

9.3. : Options for transfer of recorded data

According to Annex 1B, requirement 11, a driver can insert his DC and make printouts from the VU of any data relating to his own activities or the activities of un-named drivers.

Without a company card, he cannot make printouts of data showing the full name or card number of any driver, except where the appropriate driver card is inserted in the VU. Therefore a driver away from the company premises cannot make print-outs which, when sent back to the company, are sufficient to satisfy the requirements to store VU data in the company premises, even if printouts could meet our security requirements (see section 3.2).

If the vehicle is away from the company premises and a company card is not available at the vehicle, then it is not possible to download data from the VU except by a remote link to a place where an appropriate company card is available.

A control card can never be used for remote downloading. All remote downloading requires the use of the relevant company cards. Therefore, if a Member State or a group of companies chooses to implement a central facility for remote downloading, that central facility must have a company card. Alternatively all vehicles to be downloaded by the central facility must be locked-in by a single card rather than by a card for each separate transport company.

A company is responsible for carrying out the required downloading at the required intervals. Each company can choose to sub-contract the downloading activities, but the transport companies remain legally responsible for downloading. If a company chooses to use remote downloading, it must be on the basis that if the remote downloading is not successful at any time then the company's vehicles

must be brought to some location where an appropriate company card is available to be used for local downloading.

In a case where a company does not comply with reasonable requests for the provision of timely downloaded data, then the ultimate sanction against the company must be to remove his operator's licence. This sanction is not effective in all cases as not all companies subject to the drivers' hours rules need an operator's licence.

In principle the location of the VU or DC during downloading is unimportant.

	Charts	Print-outs – VU	Print-outs – DC	Downloading VU	Downloading DC
Driver (without company card)	Hand over Send by mail	Only driver's own data & unattributed data, Hand over, Send by mail	Complete, Hand over, Send by mail	Local downloading, Only personal data & unattributed data, Hand over, Send by mail	Local downloading, Complete, Hand over, Send by mail, transmit electronically
Transport Company without company card		Take local printout of non-attributable data	Take local printout of complete data	Local download of data not locked by any company No remote download	Local download of complete data. No remote download
Transport Company with company card		Take local printout of all company-related & non-attributable data	Take local printout of complete data	Local or remote download of data not locked by another company	Local or remote download of complete data.
Enforcement Officer	Request at roadside and at company check	Take local print-out of all data	Take local printout of complete data	Local download of all data. No remote download.	Local download of all data. No remote download.
Automatic remote downloading (performed by preprogrammed computer)	Not possible	Not possible	Not possible	Only remote download of data not locked by another company. Company card required at remote site.	Only remote download, complete data. Company card required at remote site.
Central facility with appropriate card	Not consistent with requirement to store in company premises	Take local printout of all company-related & non-attributable data	Take local printout of complete data	Only remote download of data not locked by another company using standard company card or possibly all data using 'master card'.	Only remote download, complete data. Company card or 'Master Card' required at central site.
Workshop with workshop card				Local download of all data. No remote download. May need to separate data for different companies.	

9.4. : Downloading of DC independent of a VU

A DC may be downloaded remotely by a driver (or whoever) through a card reader and appropriate infrastructure. In this case a company card is not needed.

9.5. : Downloading at a workshop

Any company requiring downloading of data from a VU may go to a workshop. However, whilst workshops may choose to offer a downloading service, they will only be required to perform downloads when carrying out repairs.

In order to satisfy enforcers requirements, the data available from the company should meet the same requirements as data available from the company following conventional downloading.

10. Concerns

controller access to data, lost data

- The mechanism to be used for protection of data passing between VU and IDE is not defined in Annex 1B.
- Without mandatory downloading, enforcers are dependent upon the help of companies to provide them with appropriate data. Data are stored in the VUs and DCs and can be left there. This situation is completely legal under the Regulation. VUs and DCs would, however, almost never be available at the time when they were needed for company checks.
- Downloading may be mandatory in some Member States but not others. This would lead to distortion of competition because in some Member States you would be able to carry out a comprehensive company check and in others company checks will be either very limited or not performed at all.
- mandatory partial downloading (e.g. only VU) would lead to a situation where data were not complete. As the Regulations currently stand, the data from voluntary manual input are only to be stored on the DC. Moreover – downloading the DC is the only sensible way to check whether a driver is driving for another company. Speed data and information regarding driving without a card, on the other hand, are only available from VUs. Only when you have data from all the relevant VUs together and the relevant DC can you create a picture of any individual driver's activities.
- During the transitional period (mixed use analogue + digital) it will become difficult to get complete data. With mandatory downloading, you will still only be able to make an efficient control if analogue data (from record sheets) are converted into a digital form and then combined with data downloaded from VUs/DCs. Only by combining the data from the two sources will drivers' activities become clear. Devices should be available which can combine analogue and digital data and these will need to be made available to enforcers.
- Data formats - After data have been downloaded they must be stored in an ESM. The precise data storage format is not fully defined in Annex 1B. Therefore there is a strong possibility that downloaded data, when offered to another organisation requiring the data, will not be readable by the second organisation. This problem may be avoided between

companies and enforcers by using the approach identified in Appendix G. However this approach is unlikely to be practicable for exchange of data between different enforcement bodies. Similarly, the format for data downloaded at a workshop is not defined.

11. Conclusions

Sub-conclusion chapter 2.1:

With the analogue tachograph, data from charts are accessible during a roadside check. With a digital tachograph, data from the DC are accessible to almost the same extent as data from charts. In addition, data are also available from the VU. Where a driver chooses not to use a chart/DC, then data from a VU will still be accessible, but will not be allocated to a specific driver. Moreover, driving without a chart is always an offence. Driving without a card is not an offence in some circumstances and will therefore be more difficult to control.

It has also to be clear that in a case where a driver has driven another vehicle earlier in that day or week, the data recorded in the VU of that previous vehicle will not be accessible to the enforcement officer. The only accessible data is that recorded on the DC, if produced, so the enforcer might not be aware of work that driver had performed without his driver card.

Sub-conclusions chapter 2.2:

From the above comparison it can be seen that, for a company check, data from charts will generally be accessible in the company. As there is currently no explicit obligation to store data from digital tachographs in the company, then data from DCs and VUs will generally not be accessible in the company.

Where drivers do not use DCs, data will still be available in VUs but it will not be allocated to a particular driver.

Data from digital tachographs will only be accessible if the company chooses voluntarily to keep a complete set of print outs or downloaded data from each DC/VU accessible in the company premises.

Sub-conclusions chapter 3.2:

There is a mismatch between the requirements for analogue and digital tachographs. For analogue tachographs the requirement to maintain and hand over record sheets is explicitly defined. For digital tachographs the detailed requirements are left to Member States to specify.

Therefore, although printouts would appear to meet the requirements of this paragraph, only downloading of the VU will fully meet the requirements. It should be noted that there is no explicit or implicit requirement for downloading of DCs.

Sub-conclusion chapter 3.3 :

The employer is responsible for his employees. In the case of hired drivers, responsibility rests with the company under whose control the driver operates.

Sub-conclusions chapter 4.5:

Detailed speed and distance information is permanently recorded on charts. Digital records of detailed speed are overwritten after 24h of driving. Therefore tracing of journey details will only be possible for the 24 hours driving that is retained in the VU.

Some data are only in the DC (e.g. any manual entries made voluntarily of activities performed when away from a vehicle). Some data are only in the VU (e.g. driving without a card, speed and overspeeding information). Data relating to an individual driver who has driven several vehicles will be spread over several VUs, possibly belonging to different companies.

Therefore, in order to check compliance with Regulations, data must be available from both from VUs and DCs.

For a roadside check the required data are accessible as the relevant DC and VU are there at the time (except where a driver has been driving without a card, in which case only data in the VU of the vehicle being checked will be available). For a company check the control officer only has access to data accessible at the company premises. Therefore information from the relevant DCs and VUs must be made accessible at the company premises. To check compliance of a specific driver, data from VUs alone are not sufficient – data are also required from DCs.

Sub-conclusion chapter 5:

Not all data related to drivers are stored in VUs – some are only stored in DCs (see section 4.3), and these data may only be available for +/- 28 days. If those data are also to be maintained for 365 days then DC contents must be either printed out or downloaded. To guarantee the required accuracy and security then downloading of DCs is the only viable option.

Sub-conclusions chapter 6.4:

Driver-related data are considered as personal data according to Directive n° 95/46/EC.

Enforcement officers must not ask for, collect, or store, more data than needed to verify compliance with the rules on driving, resting, working and availability periods.
Due to the fact that a DC may only be downloaded in its entirety, enforcement officers will get access to more data than they may legitimately use. During a roadside check there may be access to 28 days or more of activities. Directive n° 88/599/EEC only requires enforcement officers to check the last 8 to 12 days of activities.

Directive n° 95/46/EC requires controllers/enforcement officers to restrict themselves according to the principle of proportionality. Therefore the facilities provided by the driver cards for downloading may make it difficult for enforcement officers to respect the requirements of the Directive n° 95/46/EC.

The requirement according to Directive n° 88/599/EEC to check 8 to 12 days is unclear – is this a maximum or a minimum requirement ? There are differences of interpretation.

Any companies that do download and store data must be registered under data protection legislation.

To comply with data protection requirements it may be advisable to encrypt data stored in an ESM, or otherwise restrict access by unauthorised persons (for example, by requiring a password in order to access the data).

Sub-conclusion chapter 6.6:

Lock-in/lock-out and downloading of hire vehicles and allocation of data to the correct company is a problem in need of a solution.

It is proposed to encourage the users of the vehicles to use the lock-in / lock-out facilities correctly:

- to ensure that the relevant data will always be downloadable ;
- to ensure that companies prevent unauthorised persons from accessing their drivers personal data

Sub-conclusion chapter 7.4:

There would be benefit in harmonising the time allowed for collection of data for prosecutions. Given that this level of harmonisation is unlikely in any reasonable time period, there is a need to instead harmonise the period in which companies must collect data (not necessarily restricted to downloaded data).

The time allowed for collection should accommodate the most stringent Member State requirement.

Sub-conclusions chapter 7.5:

The only way to avoid loss of data in the event of equipment failure is to have those data stored (backed-up) outside that equipment. In the case of VU and DC, this can be achieved either by downloading or by taking and storing printouts. However, print-outs will not provide the required security (see section 3.2).

In the case of downloaded data, a back-up of these data should be made as an additional safeguard against loss of the downloaded data.

In the absence of an effective backup, the loss of data may be substantial.

Sub-conclusion chapter 7.10 :

Downloading of VU and DC should be undertaken at certain defined fixed moments as well as at regular intervals.

Sub-conclusion chapter 8.2:

Data from analogue tachographs must be stored in the company premises.

Final conclusions:

- when drivers use the digital tachograph there is an obvious need for downloading data for enforcement purposes ;
- downloading is preferred over producing print-outs as printouts will not meet the requirement in Regulation (EC) n° 2135/98 to guarantee the safety and accuracy of the data ;
- downloading should be performed at certain intervals and at certain defined fixed moments ;
- in order to be able to monitor compliance with Regulations (EEC) n° 3820/85, 3821/85 and Directive n° 92/6/EEC, it is necessary to have a complete record, which can only be achieved

by downloading all VUs as well as all DCs of the drivers working under the instructions of a transport company ;

- downloading of DC and VU must be mandatory ;
- there is insufficient legal basis, and no explicit requirement, in Regulation (EC) n° 2135/98 for mandatory downloading of the VU ;
- there is no legal basis at all in Regulation (EC) n° 2135/98 for mandatory downloading of the DC.

12. Proposals

what/when/how to download, changes to Regulations/Directives/Technical Annexes

12.1. : Downloading of VU and DC

- For the Vehicle Unit:

  - ✓ Immediately before permanently or temporarily transferring control of the vehicle to another person[6] or company
  - ✓ If it ceases to function correctly but can still be downloaded
  - ✓ In any case, at least every three months

- For the Driver Card :

  - ✓ Prior to overwriting of data. The 28-day period is dependent on the driving pattern of the driver and also on the memory capacity of the particular card. If, in practice, **all** driver cards have a capacity of at least 32kbytes, we recommend that the driver card be downloaded at least once every 31 days. Otherwise, we recommend that all driver cards be downloaded at least once every 21 days.
  - ✓ Before the driver leaves his/her company (that is, when a driver ceases to be employed by a company or - where companies use self-employed drivers or drivers hired from an agency - at the end of the period for which that driver is used).

- For either/both :

  - ✓ *Within 24 hours following a request by an enforcement officer involved in the investigation of a serious incident.*
  - ✓ *Within 7 days in other cases.*
  - ✓ *In any case, data will be made available to the enforcement officer within 7 days of the request.*

[6] By this we mean the transfer of a vehicle to a person acting as/or for another **transport operator** not the transfer of the vehicle to a **driver** employed by the same person or company.

12.2. : Backup system for downloaded data

- Companies should have a backup system for downloaded data : any downloaded data should be protected against accidental (or other) loss by provision of an adequate backup system.

  Enforcement officers should also have the ability to require the data to be presented

  - sorted by VRN or by driver ;
  - in the chronological order that they have been downloaded;

with file names to be clearly identifiable.

12.3. : Remote downloading

It is recommended that downloading VUs and DCs takes place remotely.

12.4. : Downloading at a workshop

Workshops are required to have facilities for downloading of VUs – though they are not required to download unless they are carrying out repairs. Workshops could therefore offer their services for regular downloading of VUs. Workshops may also choose to extend such facilities to downloading of DCs.

In order to satisfy enforcers requirements, the data available from the company should meet the same requirements as data available from the company following conventional downloading.

Appendix A : Definitions

Data – Facts relating to drivers and vehicles; facts related to the activities of drivers and vehicles. Stored in VU and/or tachograph cards

Complete data – All the data required by Regulations (EEC) n° 3820/85, 3821/85 and (EC) n° 2135/98, as well as by Directive n° 92/6/EEC together with associated amendments and Annexes.

Accessible data – Data which are available to an enforcer at an acceptable location and in a form in which he can use them

Timely data – Data which are available at the moment they are needed for enforcement purposes

Gaps – Any differences between data presented and 'complete data' as defined above

Adequate data – Accessible and timely data which are sufficient for enforcement purposes related to the need

Downloading – 'Copying, together with digital signature, of a part or of a complete set of data stored in the data memory of the vehicle or in the memory of a tachograph card. Downloading may not alter or delete any stored data.' [Annex 1B definition 's'] Downloading of the VU is normally carried out through the downloading connector at the front of the vehicle unit and with a company card inserted into the VU. Downloading of a DC can be carried out through the VU, in which case a company card is not necessary

Remote downloading – Downloading where the company card is not inserted into the VU, but is instead used via an external interface on the VU, and where the link between the VU and the external storage medium is not totally within the control of those carrying out the downloading.

Appendix B : Responsibility for compliance/temporary labour

B.1. : Past situation

ECJ Case: Auditeur du travail vs. Bernard Dufour, Crey's Interim
Article 14 (7) and (8), Regulation (EEC) n° 543/69 (= predecessor of Regulation (EEC) n° 3820/85)

Facts: a transport undertaking had hired out a driver. During a roadside check, the driver was driving without the individual control book.

Question: Who is responsible for this infringement ? Who is responsible for taking all necessary measures concerning the issue and control of the books ? The transport undertaking which had hired out the driver or the undertaking providing the temporary labour ?

One of the debates was that there was no definition of the term "undertaking" in the Regulation.

Arguments: In situation of temporary labour, the Advocate General described shortly some national systems and concluded by stating that "*the general tendency is to place the responsibility on the undertaking under whose control the driver of the vehicle performs his duties, to the exclusion of the undertaking which merely supplies labour*."

ECJ cases of Bourrasse C-228/01 and Jean-Marie Perchicot (C289-01) state that the agency supplying a hired driver may be responsible for the records of it's employee.

> As regards the management of the tachograph discs, under Article 14(1) and (2) of Regulation No 3821/85, both in its original version and in that resulting from Regulation No 2135/98, it is the employer who issues the discs to the drivers, replaces them where necessary and then retains them for at least a year.
>
> It follows that a haulage company established in one Member State, which hires out vehicles without a driver for the carriage of goods by road to a company established in another Member State, cannot retain the management of the tachograph discs of the hired vehicles.

B.2. : Solution of the ECJ

- It is the duty of the transport undertaking to ensure that the provisions of Article 14 (7) and (8) of Regulation (EEC) n° 543/69 are observed.
- The position would be different only if national legislation adopted in pursuance of Article 14 (9) of Regulation (EEC) n° 543/69 in the special case of hiring of labour were to impose that duty on the undertaking providing the temporary labour.

B.3. : Current situation

Regulation (EEC) n° 3820/85:

- Article 15 does not define the undertaking responsible ;
- Article 17 empowers Member States to adopt the necessary national dispositions.

The solution of the ECJ given in 1977 could be transposed to the current situation.

B.4. : Conclusions

Member States are competent to adopt national solutions. The interpretation of the ECJ remains valid in the case of no specific national disposition.

Appendix C : Availability of data - a comparison between today and tomorrow

Main targets of enforcers:

1. Road safety
2. Labour protection
3. Fair competition

Main targets of the company:

4. To get advantages over other companies according to the commercial competition
5. To carry out cheaper transportation
6. To get more profit

Main targets of the drivers:

7. To keep their jobs
8. To keep their social rights
9. To earn more money

To reach these targets company and driver extend the driving period and/or reduce the rest period and/or drive faster than allowed.

To reach the targets of the social Regulations and to prevent the company/drivers targets, the enforcers carry out controls in two different ways. These are company and roadside checks.

C.1. : Roadside check:

During road side check we can find information coming from:

Analogue tachograph	Digital tachograph
1) Charts 2) Tachograph 3) Further documents 4) Information from the driver	1) DC 2) VU 3) Further documents 4) Information from the driver
The number of days (charts) to control is limited by the Directive n° 88/599/EEC (most 6+1). The charts can be - read directly, - with the support of a chart reader - or through a semi- automatic evaluation (scanner/computer).	The number of days on the DC to control is limited as well by the Directive n° 88/599/EEC (most 6+1) even the DC provides +/- 28 days of data. The DC can be read through card-reader, directly through the display of the VU and/or print out.

1) The charts provide the following recorded information: - Name of the driver (by manual input) - Locations where the daily driving period started and end (by manual input) - Date (start and end of the working day) (by manual input) - VRN (Vehicle Registration Number) (by manual input) - KM of the vehicle (start and end of the working day) (by manual input) - Driving time (current week and last day of previous week) - Breaks (current week and last day of previous week) - Resting time (if recorded - current week and last day of previous week) - Other work and/or availability (written on the back of the chart) - Speed - Opening/closing the tachograph - Interruption of the electric impulses	1) The DC is providing the following recorded information: - Name (including first name) of the driver - As location only the country and in the case of Spain also the name of the region - Date (start and end of the working day) - VRN (all VRN`s driven by the driver within the last +/- 28 days) - KM of the vehicle (start and end of the working day) - The DC provides us additional information like: - Member state of the driver - Birthday and birthplace - Day of DC-issue - Validity - Issuing authority - Number of driving license - Number of DC - Photo - Signature - Optional: (Living place and space for additional national use - Driving time, of the last +/- 28 days driven on vehicles with digital tachograph. - Breaks (...+/- 28 days...) - Resting time (if DC inserted – ...+/- 28 days...) - Recording of other work and/or availability only by inserting DC into VU and switching button. No recording if away from vehicle. - No speed recording on DC - Indication of insertion/withdrawing - Interruption of the electric impulses
Possible manipulation of the chart: - Driving without chart - Putting no information on the chart - Putting wrong information on the charts (wrong name, locations, KM etc.) - Driving with different/several charts - Manual manipulation of the charts (with circle	Possible manipulation of the DC: - Driving without DC - Putting no information manually on the DC (manual input) - Putting wrong information about locations (the country and in the case of Spain also the name of the region - situation will change if manual input into force) - Putting further wrong information by manual input - Driving with different/several DC - Manipulation of data (by breaking the

etc.) - "Loosing" the charts - etc…	keys…) - "Loosing" the DC - Erasing data on the DC through abnormal circumstances - etc…
2) The Tachograph provides the following information: - Odometer (KM) - Correct calibration - Last periodical control of the Tachograph - Presence of the sealings of the Tachograph	2) The VU provides the following information: - Odometer (KM) - Correct calibration - Last periodical control of the VU - Presence of the sealings of the VU - Speed (per second for the last 24 hours vehicle operating plus over speeding for the time before) - Driving time (+/- 365 days vehicle related). - Breaks (+/- 365 days vehicle related) - Rest time (if recorded +/- 365 days vehicle related) - Any movement of the vehicle without or damaged DC - Interruption of the electric impulses - Indications of Number of the driver card (dates and hours of insertion and withdrawing) - Number of any card (COC, CC, WC etc…) inserted into the VU within the last +/- 365 days - Any disturbance of the tachograph system (sensor, VU, DC) with indication of date and time - Change of time with date, time and DC-Number - Status of the driving (single or multiple)
	The printout from the VU provides us more or less the same information as the VU

Possible manipulation of the Tachograph: - Manipulation of the Tachograph itself (unallowed opening, bending writer parts, wrong calibration, stopping/interrupting the clock, modifying the impulse etc…) - etc…	Possible manipulation of the VU: - Manipulation of the VU itself (wrong calibration, stopping/interrupting the power, modifying the impulse, wrong VRN etc…) - "Stolen" VU - Exchanging VU without downloading data from previous VU - Erasing data on the VU through abnormal circumstances - Manipulation of data within the VU (theoretical possibility) - etc…
3) From the further documents we get the following information: - Identification of the Haulier/Company - Nature of the transported Goods - Locations of loading and unloading - Identification of the vehicle - Legal/contract relation between driver and company - Transport license	3) From the further documents we get the following information: - Identification of the Haulier/Company - Nature of the transported Goods - Locations of loading and unloading - Identification of the vehicle - Legal/contract relation between driver and company - Transport licence
Possible manipulation of documents: - False documents - etc…	Possible manipulation of documents: - False documents - etc…
4) The driver will provide the following information: - Identification of his person - Driver license - Relevant holidays/vacation/sickness/no driving within scope etc…	4) The driver will provide the following information: - Identification of his person - Driver license - Relevant holidays/vacation/sickness/no driving within scope etc…
Possible manipulation of the driver info.: - False documents - False explanations/statements - etc…	Possible manipulation of the driver info.: - False documents - False explanations/statements - etc…
There is further important information, which is needed for enforcement purposes but not recorded on the charts or proven by further documents - such as daily and weekly rest. These periods of non-recording are usually interpreted as rests.	There is further important information, which is needed for enforcement purposes but not recorded on the DC and/or VU or proven by further documents - such as daily and weekly rest. These periods of non-recording are usually interpreted as rests.

C.2. : Company check:

During company check we can find information coming from:

1) Charts (driver related, including the charts themselves) 2) Tachograph 3) Further documents provided by the undertaking	1) DC (data available only if downloaded – but in this case driver related) 2) VU (data available on the base of voluntarily downloading or presentation of the vehicle(s) with VU but in this case vehicle related) 3) Further documents provided by the undertaking
According to Regulation (EEC) n° 3821/85 modified (Article 15) the company has to keep the records for +/- 365 days for enforcement purposes. The charts can be read directly, with the support of a Chart reader or through a semi- automatic evaluation (scanner/computer).	According to Regulation (EEC) n° 3821/85 modified (Article 15) the company has to keep the records for +/- 365 days for enforcement purposes. The records can be read directly from the equipment (hard/software) provided by the company or the enforcers.
1) The charts are providing the following recorded information: - Name of the driver - Locations where the daily driving period started and end - Date (start and end of the working day) - VRN (Vehicle Registration Number) - KM of the vehicle (start and end of the working day) - Driving time, driver related of the last +/- 365	1) If the data from the DC are downloaded the following recorded information are provided: - Name (including first name) of the driver - As location only the country and in the case of Spain also the name of the region (situation will change if manual input in to force). - Date (start and end of the working day) - VRN (all VRN`s driven by the driver within the last +/- 28 days) - KM of the vehicle (start and end of the working day) - The DC contents additional information as: - Member state of the driver - Birthday and birthplace - Day of DC-issue - Validity - Issuing authority - Number of driving license - Number of DC - Photo - Signature - Optional: (Living place and space for additional national use - Driving time, driver related of the last 365 days driven on vehicles with digital

days driven on vehicles with analog tachograph - Breaks (+/-365 days…) - Resting time (+/- 365 days… if chart inserted) - Other work and/or availability (written on the back of the chart) - Speed - Opening/closing the tachograph - Interruption of the electric impulses	tachograph. - Breaks (+/- 365 days…) - Resting time (+/- 365 days… if DC inserted) - Other work and/or availability only if DC was inserted into VU and correct button used. No recorded data if away from vehicle. (Situation will change if manual input in to force). - Indication of insertion/withdrawing - Interruption of the electric impulses
Possible manipulation of the chart: - Missing charts - Charts without any information - Charts with wrong information (name, locations, km, etc...) - Charts indicating manual manipulation (with circle….) - Charts indicating manipulation of the tachograph - Data coming from charts used by one driver with different names - etc…	Possible manipulation of the data from DC`s/VU`s: - Missing data (e.g. no recording of other work/availability, "lost" data through abnormal circumstances, "lost" DC / "stolen" VU, no or not complete downloading, - Wrong locations (only the country and in the case of Spain also the name of the region - situation will change if manual input into force) - Wrong data if manual input into force - Manipulated data (by broken keys…) - Data coming from different/several DC`s used by one driver - etc…
2) The Tachograph is not available during company checks:	2) If the data from the VU are downloaded the following recorded information are provided: - Odometer (KM) - Correct calibration - Last periodical control of the VU - Speed (per second for the last 24 hours vehicle operating plus over speeding for the time before) - Driving time (vehicle related) - Breaks (vehicle related) - Rest time (if recorded vehicle related) - Any movement of the vehicle without or damaged DC - Interruption of the electric impulses - Indications of Number of all driver cards used in this vehicle (dates and hours of insertion and withdrawing)

	- Numbers of all other cards (COC, CC, WC) inserted into the VU within the last +/- 365 days - Any disturbance of the tachograph system (sensor, VU, DC) with indication of date and time - Change of time with date, time and relevant DC-Number - Driving status (single or multiple) - Cross-checking all VUs with DC('s)
Possible manipulation of the tachograph:	Possible manipulation of the VU - If there is no downloading the vehicle(s) has to be presented for company check (see roadside check)
3) The further documents provided by the undertaking (List of employees, vacation list of drivers, payroll, disposition of journeys etc...) get the following information: - Locations of loading and unloading - Identification of the vehicle - Legal/contract relation between driver and company - Transport licence - Cross-checking the provided documents with charts or other information	3) The further documents provided by the undertaking (List of employees, vacation list of drivers, payroll, disposition of journeys etc...) get the following information: - Locations of loading and unloading - Identification of the vehicle - Legal/contract relation between driver and company - Transport licence - Cross-checking the provided documents with available data or other information
Possibilities of manipulations: - False documents - etc…	Possibilities of manipulations: - False documents - etc…

There is further important information, which is needed for enforcement purposes but not recorded on the charts/DC or proven by further documents - such as daily and weekly rest. These periods of non-recording are usually interpreted as rests.

Appendix D : Security Mechanisms

D.1 : Background

Reasons for downloading of data from a vehicle unit (VU) or a tachograph card:

- to maintain a continuous record of driver and vehicle activities after the VU/card memory has been filled and old data is being over-written
- to collect data together to allow analysis over multiple cards and/or vehicles
- to make available at a central point data from VUs and cards whilst the VUs and cards themselves are not available. Cards/VUs may be in use elsewhere. They may be faulty. VUs may have been sold or scrapped.

The continuous record is required at a central point:

- for fleet management purposes
- to allow the possibility of company checks by enforcement officers.

D.2 : Basic security mechanisms

The objectives of the security relating to downloaded data are:

- to ensure that downloaded data cannot be changed after it has been downloaded
- to be able to prove that the data came from the VU/card as claimed.

To achieve these objectives, the data are protected by the addition of digital signatures. A signature is generated by compressing ('hashing') the data to a manageable size, and then encrypting the result. The signature is then added to the end of the data and stored with the data.

It is important to note that privacy of the data is not considered a security issue and therefore the data itself is not hidden by encryption.

D.3 : Choice of encryption mechanisms

When choosing encryption mechanisms for any given purpose, there are a number of considerations:

- strength of security required
- implications if the security is compromised (broken)
- the time taken to encrypt/decrypt data

In the case of the tachograph application, the security requirements have been divided into two. Some data are in effect transient (e.g. data transfers between card and VU during operation) and other data

require long-term protection. Conversely, more time can be allowed for generation of the signatures for blocks of downloaded data, whilst it is important to minimise the security-related delays during normal operation when many secured messages are being exchanged.

Thus two separate security mechanisms have been selected for the tachograph application:

- public key (RSA) for long-term protection of data. This is also used for authentication of data (proving that the data is genuine). This also has the benefit that if one equipment key pair is identified ('broken') then the remaining key pairs remain valid and secure.
- Private key (DES-based) for transient data. Any key based on DES is used for a maximum of 240 data exchanges, and then the key is changed.

D.4 : Key Management

In the tachograph application, encryption based on DES is only used for transient data. The keys are generated by the equipment as needed, and are changed regularly. There is therefore no requirement for external generation and distribution of these keys.

Public key encryption is based on key pairs. One key, the public key, is generally available. The security is based on the difficulty of identifying the matching private key that (in principle) is only known in one place. Every entity in the greater tachograph system – authority, equipment etc… – has its own key pair. A mechanism is required to generate and store these key pairs securely (hence the high-level discussions of key management). Furthermore, a mechanism is required to allow keys explicitly to be identified as valid, otherwise anyone with a little knowledge could generate his own apparently valid key pairs.

The method selected to identify keys as valid is to have a hierarchy of keys. The public key of an equipment is signed (encrypted) using the private key of the relevant Member State. Thus if the public key of the Member State is known then the public key of the equipment can be identified as genuine.

At the level above in the hierarchy, it is important to be able to confirm that the Member State public key is valid. Therefore the public key of the Member State is signed (encrypted) using the European-level private key. Knowing the European public key, the Member State public key can be validated.

There then remains a need to identify the validity (or otherwise) of the European public key. There is no higher level in the hierarchy – this key must be obtained direct from a trusted source.

D.5 : Certification Authorities

Within the Annex 1 B of Regulation (EEC) n° 3821/85 as last amended the need for a European Certification Authority is identified (but the actual authority is not identified). This authority will generate the European key pair, retaining as secret the private key and making available to others the public key as required. It will then use the European private key to certify the public key of each Member State, and will keep records of all certified keys.

At the next lower level, each Member State must have a Certification Authority. Clearly this can be subcontracted in an appropriately controlled manner, and there is no particular reason why the subcontracted organisation necessarily needs to be within that Member State. Each Member State Certification Authority will maintain that Member State's key pair and will use their private key to certify the public key of every equipment originating in their country. The equipments involved are all the tachograph cards issued in that country and also all vehicle units etc… originating in that country.

From the above, it can be seen that the European Certification Authority is a very important part of this chain. However that authority has a very modest amount of work to do - maintain the European key pair and record the certificates of 15 Member States plus any others which join in the future. Each Member State Certification Authority has a much greater task in that the number of certificates to be signed and recorded is much larger - a new certificate will be needed each time a new card or vehicle equipment is issued.

D.6 : Construction of an Equipment and a Member State Certificate

The certificate of an equipment is built up as in the following diagram.

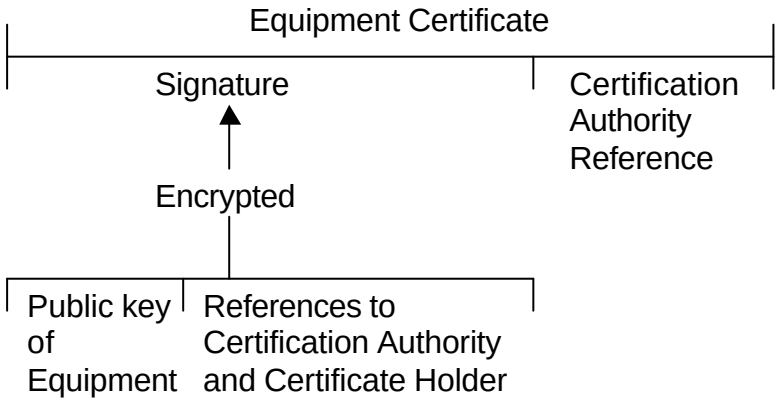

Fig.1 Construction of Equipment Certificate

For an equipment, the encryption is carried out using the Member State private Key.

A Member State certificate is built up in the same way, except that the public key to be signed is that of the Member State and the encryption is carried out with the European private key.

D.7 : Construction of Signature attached to downloaded data

Each block of downloaded data has a signature attached. This signature is built as in the Fig. 2. The data block (unencrypted) is stored together with the signature.

To be able to check that the signature is valid, it is essential to know the equipment public key and to be sure that it is valid. This is achieved by storing the equipment signature with the data and signature. Similarly, to allow the equipment signature to be validated, the appropriate member state certificate is also stored with the downloaded data and signatures.

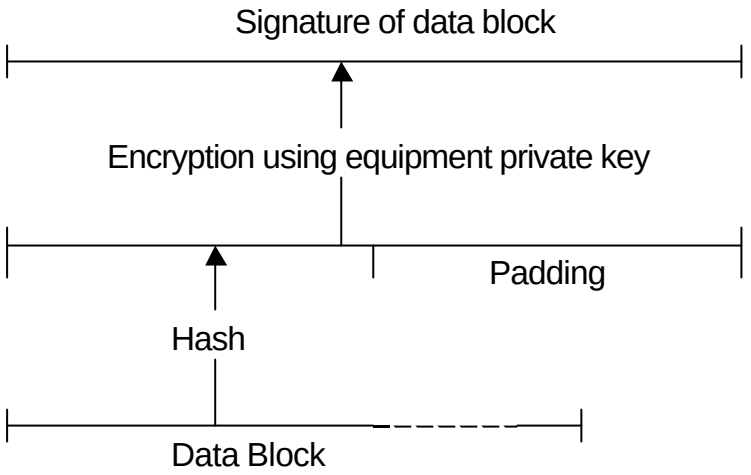

Fig.2 Construction downloaded data signature

Several blocks of data will probably be downloaded in one downloading session, particularly when downloading from a VU. Annex 1B requires all data downloaded in one session to be stored together in one file with a structure shown in Fig. 3.

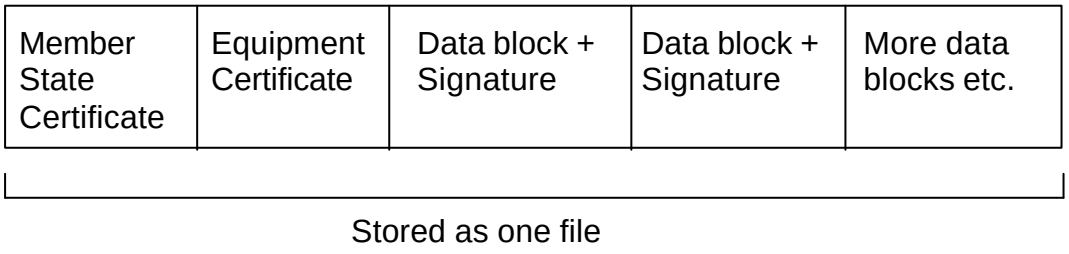

Fig. 3 Storage of downloaded data

D.8 : Validation process for a downloaded block of data

1. Recover the Member State public key from the Member State certificate. Note: this requires the European Public key which must be received from a trusted source.
2. Using the Member State public key, recover the equipment public key from the equipment certificate.
3. Perform a hash of the data in the data block to be validated.
4. Using the equipment public key, recover the hash value which was computed by the equipment and stored in the signature.
5. Compare the hash value stored in the signature with the hash value computed from the data to be validated. If the two hash values are the same then the data is valid.

In practice this process will be carried out using a software package running on a PC or equivalent. The only thing which needs to be known is the European public key. In practical terms, it will generally be preferable to use a tachograph card to carry out the encryption/decryption functions as these cards have built-in specialist hardware to speed up such computations. Thus the software package will generally run in conjunction with a tachograph card. If this card is a trusted control card and it contains a trusted copy of the European public key, then the whole validation process can be automated.

For further authentication of the data, the equipment and Member State certificates contain further data relating to the authority that issued the certificate(s) and to the authority holding the certificate(s). These can be traced back to further confirm the validity of the certificates. As every certificate should be unique, they also give the possibility of identifying multiple use of key pairs which would indicate fraud.

Appendix E : Data protection and digital signatures vs. Digital tachograph

Downloading of data, in the framework of the Regulation (EEC) n° 3821/85 as last amended by Regulation (EC) n° 2135/98, leads to some interrogations regarding the rules established on one side by the Directive n° 95/46/EC on the protection of individuals with regard to the processing of personal data and of the free movement of such data[7], and, on the other side, by the Directive n° 1999/93/EC on a Community framework for electronic signatures[8].

The objective is not to define, in depth, the conditions under which the downloading of data stored on a driver card (DC) or in a vehicle unit (VU) would respect the provisions of the two Directives mentioned above. But it is to give some guidelines on what will have to be taken into consideration at the time of implementing the digital tachograph in EU Member States.

E.1 : Downloading and data protection

The Directive n° 95/46/EC has been adopted at the European level in order to give a minimum legal framework to the different EU Member States, at a time where a relatively important number of these Member States did not have any rules regulating data protection.

Nevertheless, the provisions of the Directive n° 95/46/EC are not totally new. They are inspired by the Convention n° 108 of the Council of Europe adopted in 1981, which are closed to the provisions of the Guidelines adopted by OECD in 1980, themselves being very closed of the provisions of the first French law on data protection adopted in 1976. These texts are also in accordance with the Guidelines adopted by the United Nations in 1990.

In other words, there is currently a world-wide consensus on what has to be the protection of personal data.

1-1) Some important definitions

In this Directive, some important definitions are given :

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

7 OJEC n° L 281, 23-11-1995, page 31
8 OJEC n° L 13, 19-01-2000, page 12

This definition is very broad and leaves no doubt on the fact that the data recorded by the tachograph, in the VU as well as on the DC, are personal to the driver. The word "personal" are referring later on in this definition to the words "natural person". Therefore, it has to be pointed out once more time : the rules concerning personal data concern individuals, and not legal persons, such as companies, administrations, etc…

- *processing of personal data : shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

Downloading, in our case, could be considered as a kind of "dissemination", if we consider that the data recorded and stored into the VU and on the DC, are disseminated in the companies', service providers' or enforcement officers' PCs.

- *Personal data filing system : shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.*

These provisions are wide enough to embrace downloading wherever are the data, in EU Member States, in the companies, in their sister companies when it is the case, kept by ad hoc service providers, etc …

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

In other words, the EU Member States have the possibility to adopt national rules defining on which way data will have to be stored and presented to the controllers during company checks.

1-2) Principles relating to data quality

The Directive n° 95/46/EC, in its Article 6 states that data must be :

- *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.*

This principle is very important and is the one – with the following one presented below - that causes the very big majority of the problems to the national authorities and to the controllers. The temptation is important to do more with the data collected than only what should be done according to the provisions of the EU Regulations and/or the national law to which they refer.

- *adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This principle is linked to the previous one, in the sense that to control the (EEC) Regulation n° 3820/85, the enforcement officers do not have to ask more data than those needed to verify the respect of driving, resting, working and availability times.*

It is common to speak in that case of the principle of proportionality.

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

Which means that enforcement officers who would like to keep the data for more than what can be considered as acceptable according to the Regulation (EEC) n° 3820/85 (one year), would have to adopt specific national rules. It could be the case for the enforcement officers who are currently using the diagram charts for checking salaries and not only driving, resting, working and availability times and who would like to continue to do the same thing with the downloaded data.

The fact that the data have to be kept in a form which permits identification of data subjects does not mean that data will have absolutely to be drivers related. It just means that whatever will be their form, they will have to allow enforcement officers to have access to the drivers names.

1-3) Criteria for making data processing legitimate

Article 7 of the Directive n° 95/46/EC states that personal data may be processed only if:

- *it is necessary for compliance with a legal obligation to which the controller is subject;*
- *it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed ;*
- *[…].*

In other words, if the provisions of Article 6 described above are respected, Article 7 gives the possibility to the controller to process any data necessary to check compliance of drivers and companies activities with the Regulation (EEC) n° 3820/85.

1-4) Information to be given to the data subject

It is indirectly recommended by Article 11 of the Directive n° 95/46/EC to the Member States, to issue a national law in which the downloading of data will be clearly defined, in the sense that it has to be stated that the data downloaded will notably concern drivers, and that these data could be downloaded from companies for which they have worked, to enforcement officers.

Otherwise, in absence of such a precision, Article 11-1 would force the companies in some circumstances to inform the drivers concerned by the downloading, of the control performed, of the data downloaded, etc … Which is not the case if downloading is foreseen in the national law and described in such a way that it is clear for the drivers as well as for operators, that data are going to be collected by enforcement officers regularly and/or on request.

Such a precision could obviously avoid legal actions from drivers against operators.

1-5) Security of processing

Article 17 states that Member States shall provide that the enforcement officers must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

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

The Directive n° 95/46/EC confirms the necessity to implement secure means whenever data have to be processed, without presuming the technical solutions to be implemented.

1-6) Transfer of personal data to third countries

Article 25 of the Directive n° 95/46/EC states that the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

This Article will have to be taken into account each time a EU Member State will have to transfer data to a third AETR country.

E.2 : Downloading and electronic signatures

According to Article 1 of the Directive n° 1999/93/EC of 13 December 1999, on a Community framework for electronic signatures[9], the purpose of this legal text is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic

9 OJEC n° L 13, 19-01-2000, page 12

signatures and certain certification-services in order to ensure the proper functioning of the internal market.

In this Directive, electronic signature means data in electronic form which are attached to or logically attached with other electronic data and which serve as a method of authentication (Article 2, 1). Therefore, the Directive does not contradict the provisions of the Regulation (EC) n° 2135/98 and most especially those of its technical annex.

The only provisions which have to draw our attention in the framework of this report, are those of Article 5 concerning the legal effects of electronic signatures. It is indeed stated that Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

- satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data, and
- are admissible as evidence in legal proceedings.

Member States shall also ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

See also the Final report on data protection.

Appendix F : Localisation of a transport company

Which location of a multi-sites transport company should be responsible for storing the data (centrally) and monitoring compliance of Regulations (EEC) n° 3820/85 and 3821/85 ?

F.1 : Situation in EU law: general considerations

There are some references on this question in EU law:

- Right of establishment (article 48 of the EC Treaty);
- Competition rules: notion of enterprise which can be considered as an economic entity (Article 81 of the EC Treaty).

The EC Treaty is taking into account the different conceptions of the Member States and considers equally the different criteria used in the European countries.

Therefore, article 48 EC describes which firms shall benefit the same treatment as natural persons, who are nationals of Member States and takes into account many criteria that are applicable at national level in the Member States. Article 48 deals with "companies or firms formed in accordance with the law of a Member State" that have "their registered office, central administration or principal place of business within the Community".

At national level, there are rules for the determination of the localisation of the company. Amongst the Member States, different concepts are used:

- incorporation criteria: registered office as mentioned in the statutes of the company (used in UK, Ireland, Denmark, The Netherlands);
- effective head office: place where the decisions with regard to the activities are taken/centre of activities (used in France, Portugal, Spain, Greece).

The rules of competition are very pragmatic and the European Court of Justice has considered the economic definition of an undertaking. What is the most important is the risk of distortion of competition within the common market.

F.2 : Situation in EU law : specific cases

In some specific cases the European Directives or Regulations determine the place of establishment.

There is a recent example with Directive n° 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the internal market (OJEC, n° L 178/2000).

Recital n° 19: actual pursuit of an economic activity
"In case where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service."

In the case of Regulation (EEC) n° 3820/85, the text does not deal with this question. In the absence of provisions determining the localisation of the responsible transport company, the national laws of the Members States are applicable; different concepts are then applicable.

Appendix G : Access to downloaded data

G.1. : The Regulations

The relevant text is the following:

Main Body Chapter I. DEFINITIONS

s) "downloading" means:
copying together with digital signature of a part or of a complete set of data stored in the data memory of the vehicle or in the memory of a tachograph card;
Downloading may not alter or delete any stored data.

Main Body Chapter III. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR RECORDING EQUIPMENT

18. Data downloading to external media

149 The recording equipment shall be able to download on request data from its data memory or from a driver card to external storage media via the calibration/downloading connector.

150 In addition and as an optional feature, the recording equipment may, in any mode of operation, download data through another connector to a company authenticated through this channel. In such a case, company mode data access rights shall apply to this download.

151 Downloading shall not alter or delete any stored data.
The calibration/downloading connector electrical interface is specified in Appendix 6.
Downloading protocols are specified in Appendix 7.

Appendix 7. Data downloading protocols

This appendix specifies the procedures to follow in order to perform the different types of data download to an External Storage Media, together with the protocols that must be implemented to assure the correct data transfer and the full compatibility of the downloaded data format to allow any controller to inspect these data and be able to control their authenticity and their integrity before analysing them.

1.1 Scope

Data may be downloaded to an ESM [External Storage Medium]:

- *from a Vehicle Unit by an Intelligent Dedicated Equipment (IDE) connected to the VU,*
- *from a tachograph card by an IDE fitted with a card interface device (IFD),*
- *from a tachograph card via a vehicle unit by an Intelligent Dedicated Equipment (IDE) connected to the VU.*

To give the possibility to verify the authenticity and integrity of downloaded data stored on an ESM, data is downloaded with a signature appended in accordance with Appendix 11 common security mechanisms. The source equipment (VU or card) identification and its security certificates (Member state and equipment) are also downloaded. The verifier of the data must possess independently a trusted European public key.

DDP_001 Data downloaded during one download session must be stored in the ESM within one file. The file name shall have a maximum length of 8 characters and its extension a maximum length of 3 characters.

2. V.U. data downloading

2.3 ESM File storage

DDP_034 When a download session has included a VU data transfer, the IDE shall store within one physical file all data received from the VU during the download session from "Positive Response Request Upload" included up to "Positive Response Transfer Exit" excluded. Data stored excludes message headers, sub-message counters, empty sub-messages and checksums but include the LID and SID (of the first sub-message only if several sub-messages).

3. Tachograph cards downloading protocol

3.4 Data storage format

3.4.1 Introduction

DDP_040 The downloaded data has to be stored according to the following conditions:
- *The data shall be stored transparent. This means that the order of the bytes as well as the order of the bits inside the byte that are transferred from the card has to be preserved during storage.*
- *All files of the card downloaded within a download session are stored in one file on the ESM.*

3.4.2 File format

DDP_041 The file format is a concatenation of several TLV [Tag Length Value] objects.
DDP_042 The tag for an EF [Elementary File] shall be the FID[File Identifier] plus the appendix „00".

DDP_043 *The tag of an EF's signature shall be the FID of the file plus the appendix „01".*

DDP_044 *The length is a two byte value. The value defines the number of bytes in the value field. The value „FF FF" in the length field is reserved for future use.*

DDP_045 *When a file is not downloaded nothing related to the file shall be stored (no tag and no zero length).*

DDP_046 *A signature shall be stored as the next TLV object directly after the TLV object that contains the data of the file.*

Definition	Meaning	Length
FID (2 Bytes) || „00"	Tag for EF (FID)	3 Bytes
FID (2 Bytes) || „01"	Tag for Signature of EF(FID)	3 Bytes
xx xx	Length of Value field	2 Bytes

Example of data in a download file on an ESM:

Tag	Length	Value
00 02 00	00 11	Data of EF ICC
C1 00 00	00 CE	Data of EF Card_Certificate
		...
05 05 00	09 DA	Data of EF Vehicles_Used
05 05 01	00 80	Signature of EF Vehicles_Used

G.2. : Options for ESM

Nothing in the Regulation specifies exactly what an 'ESM' is, only that it is an external storage medium. Intentionally the details of this device are left open. The following is a (non-exhaustive) list of potential external storage media:

Storage contained within or permanently connected to:

- PC running DOS, Windows, Linux
- Apple Macintosh
- 'Mainframe' e.g. IBM
- Internet Server, e.g. Sun Server
- A dedicated device designed specifically as a combined IDE/ESM for tachograph applications
- Future devices/operating systems

Storage devices:

- Floppy disk – size 8", 5¼", 3½", 3", which format?
- Tape – what size/type? What format?
- CDROM – what format?

- PCMCIA memory card – what format?
- Flash Disk – what format?
- Future storage devices

In addition the data/files may be managed by a database system for easy reference and retrieval. This is very likely to happen in larger organisations or where storage of downloaded data is carried out by a third party offering such a service. Which database system will be used? Alternatively the files may be managed by file names (maybe sequential or random) and a log book.

Given the range of possible storage arrangements for the data, the restriction of file names to the '8.3' format (requirement DDP_001) seems totally irrelevant.

G.3. : The Real Data Storage Requirements

- Data must be stored reliably such that what is later recovered is exactly what was stored.
- Records must be complete so that a complete history is available.
- The stored data must be made available to enforcement officers in a form in which they can use it and at a location where they can receive it.
- Stored data files must be sufficiently identified such that it is possible to satisfy requests for data relating to specific drivers/vehicles and specific dates.
- The data must be made available at the time when it is needed (or at least within an acceptable time after it has been requested).

Clearly the exact storage medium used for storage and the file names used are of no consequence to an enforcement officer provided he has access to the data in a form in which he can use it. Conversely, presenting a enforcement officer with an 8" floppy disk which genuinely holds the data but for which the control officer does not have the correct equipment is no good.

Considering these 'real' requirements again, there is nothing that really constrains where and how data is stored.

G.4. : Proposal for a common way of presenting data to an enforcement officer

The only way of making download data available which is well specified in Annex 1B (apart from reading direct from a tachograph card) is the download interface specified in Appendix 6 (connector and signal voltage levels etc...) and Appendix 7 (data download protocol).

Enforcement officers will need equipment and software to download from the vehicle unit in accordance with Appendices 6 and 7. Thus, if the store of downloaded data has an interface that can operate in the same way as the download interface on a VU, there will be no need for additional equipment to be able to accept downloaded data.

Appendix 7 specifies that all data received from the VU during downloading shall be stored exactly as it is received. This specifically includes all digital signatures. There is therefore no need for the equipment that is to supply previously downloaded data to know anything about the security algorithms etc... They are already stored with the data and can be repeated as needed within the downloading protocol.

One aspect of the specifications in Appendices 6 and 7 that would be inconvenient would be the connector specified in Appendix 6. This is fine for the front of the VU and perhaps for a purpose-designed downloading unit. For any more general computer equipment this connector would not normally be available. Almost all computers do, however, have a serial data connector according to RS232. This is exactly as specified in Appendix 6 apart from the connector itself. It would be simple to provide an alternative cable or simple adapter to allow connection to the data storage equipment (especially as the IDE will generally be based on a standard computer with a standard RS232 data connection).

G.5. : Benefits of the proposal

- The means and details of data storage become unimportant. Any convenient storage medium may be used including any to be identified in the future.
- The required protocols are already specified in Annex 1B. Other than agreeing on the use of an alternative connector (which is already well specified in the computer industry) there is no need for any further specifications.
- The location of the store for downloaded data becomes unimportant. Data may be stored remotely if appropriate, so long as access to the data is available at a point convenient for the company and the control officer.
- The precise means of access to the data is exactly as already needed by control officers and others for downloading from a VU. No extra equipment is required.

G.6. : Possible disadvantage of the proposal

- Putting a floppy disk or CDROM of an acceptable format into a control officer's PC is quick. Using a downloading interface may take a minute or two (but no longer than it takes to download from a VU).

Appendix H : Company lock-in/lock-out

In Requirements 051 - 055 of Annex 1B to Regulation (EC) n° 2135/98 the company locks management has been described.

The digital tachograph/VU offers companies the possibility to lock their data. A company may lock its old data by inserting their company card at the beginning of the use of a vehicle/VU (moment of lock-in). The locking of data will prevent other companies of having access to data to which they are not entitled. This is, however, a responsibility of companies themselves. After insertion of a company card of another company, data will automatically be locked again (moment of lock-out).

In principle only that company will have access to its "old" data (i.e. data which are locked-out) with the company card of the first mentioned company. After 20 locks, however, data will not any longer be locked; they are accessible by any person [with a company, workshop or controller card] (requirement 104 of Annex 1B).

Data will anyway always be accessible for enforcement officers and for workshops.

Appendix I : Equipment Required

infrastructure, costs

I.1. For Enforcement Officers – minimum

- Plenty of paper for print-outs

I.2. For Enforcement Officers – preferred

- Laptop computer, dedicated equipment or whatever with appropriate connection to VUs
- External Storage Medium (ESM) which may be part of the laptop computer above
- Hand-held card reader
- Extra paper roll for print-outs
- Software for analysis of downloaded data
- Scanners for Annex 1 charts and perhaps also for Annex 1B print-outs

I.3. Transport Companies

- Hardware (laptop computer, dedicated equipment or whatever) with appropriate connection to VUs
- Card reader (hand-held of office)
- Software for analysis of downloaded data
- Storage and backup facilities for downloaded data
- Appropriate remote link and hardware for remote downloading

I.4. Workshops

- Hardware with appropriate connection to VUs
- Card reader
- Storage and back-up facilities for downloaded data
- Appropriate remote link and hardware for remote downloading

I.5. Other infrastructure

- To be specified by industry

I.6. Downloading Centre

- Master Card
- Appropriate hardware etc. for remote downloading
- Storage and backup facilities for downloaded data
- Software for analysis of downloaded data, e.g. to identify data relating to individual drivers from records from many VUs.

Links (or whatever) to allow transport companies and enforcement agencies to gain access to data.