

RECOMMENDATIONS

COMMISSION

COMMISSION RECOMMENDATION

of 23 January 2009

on guidelines for best enforcement practice concerning checks of recording equipment to be carried out at roadside checks and by authorised workshops*(notified under document number C(2009) 108)***(Text with EEA relevance)**

(2009/60/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to Directive 2006/22/EC of the European Parliament and of the Council of 15 March 2006 on minimum conditions for the implementation of Council Regulation (EEC) No 3820/85 and (EEC) No 3821/85 concerning social legislation relating to road transport activities and repealing Council Directive 88/599/EEC ⁽¹⁾, and in particular Article 11(1) thereof,

Whereas:

- (1) Pursuant to Article 11(1) of Directive 2006/22/EC, the Commission is to establish guidelines on best enforcement practice concerning the checks of vehicles to be carried out by control officers either at the roadside, or at the premises of undertakings, or by authorised workshops and fitters.
- (2) Recording equipment in road transport is necessary to indicate the periods of time that drivers spend driving and resting, and also to ensure that effective checks of social legislation in road transport can be carried out by the competent national control bodies.
- (3) To ensure that such recording equipment functions correctly and reliably, and that the recording and storing of data can be guaranteed, periodic checks and inspections are necessary after the recording equipment has been installed.
- (4) However, periodic checks and inspections do not appear to occur with a frequency likely to effectively deter those drivers and operators who seek to abuse the system by using manipulation devices or other similar means.
- (5) Research and information from experts have established that attempts to defraud the tachograph system have been widespread in vehicles equipped with analogue tachographs; similar attacks and threats are now being made to the digital tachograph system.
- (6) The same research has shown that a number of manipulations are possible and known to exist in the road transport sector to attempt to defraud the tachograph, in particular the digital tachograph system.
- (7) Such attempts and threats pose a serious risk to road safety and also have unacceptable negative impacts on fair competition and on the social conditions of drivers in road transport.
- (8) As a result of the improved security of the digital tachograph as opposed to the analogue tachograph, threats and attempted attacks to the system can be more easily detected, so that the risk of unscrupulous drivers and operators being caught with such devices is accordingly increased and should act as a significant deterrent.

⁽¹⁾ OJ L 102, 11.4.2006, p. 35.

- (9) This Recommendation accordingly aims to encourage and support Member States in adopting procedures and methods that, based on research and technical expertise from the industry, will considerably improve the possibilities of preventing and detecting such attempted fraud.
- (10) In particular, this Recommendation sets out best enforcement practice, as identified in research carried out by the Joint Research Centre.
- (11) This Recommendation forms, together with a proposed Directive on additional checks to be carried out at the roadside, a package of enforcement measures that aim to considerably improve the detection and prevention of devices used to defraud the digital tachograph system.
- (12) The measures provided for in this Recommendation are in accordance with the opinion of the Committee set up by Article 18(1) of Council Regulation (EEC) No 3821/85 ⁽¹⁾,

HEREBY RECOMMENDS:

1. Adopt and apply the best practice guidelines set out in the Annex to this Recommendation concerning the checks on vehicles to be carried out by control officers at the roadside or at the premises of undertakings, or by fitters and technicians at workshops approved by the competent authority of the Member State, in order to detect and prevent the use of manipulation devices in recording equipment used in road transport.
2. Apply these guidelines, where appropriate, in the context of the national enforcement strategies referred to in Article 2 of Directive 2006/22/EC.

Done at Brussels, 23 January 2009.

For the Commission
Antonio TAJANI
Vice-President

⁽¹⁾ OJ L 370, 31.12.1985, p. 8.

ANNEX

RECOMMENDATIONS ON COUNTERMEASURES TO BE ADOPTED BY MEMBER STATES TO DETECT AND PREVENT THE USE OF MANIPULATION DEVICES

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

CHAPTER 2: EFFECTIVE ROADSIDE CHECKS

- A. Organisation and equipment
- B. Double check points methods with analysis of real speed and distance of vehicles
- C. Single check point methods based on detailed analysis of downloaded data
- D. Single check point methods based on technical control of seals
- E. Directing the vehicle to a workshop
- F. Checking vehicles or data at company remise

CHAPTER 3: TRAINING AND BEST PRACTICE

CHAPTER 4: WORKSHOP INSPECTIONS

- A. Legal Base
- B. Broken or Absent Seals
- C. Analysis of Data Records
- D. Control of Pairing Between Motion Sensor and Vehicle Unit
- E. Special Procedures as a Result of a Roadside Check

CHAPTER 5: REPORT AND AUDIT OF WORKSHOPS

CHAPTER 6: FINAL PROVISIONS

Chapter 1: Introduction

- 1.1. This Commission Recommendation describes what Member States could be encouraged to do in order to meet the threats posed by the use of manipulation devices in tachographs and at the same time to promote and support preventative countermeasures amongst Member States to deal with those threats.

- 1.2. The presence of manipulation devices in vehicles intended to interfere with the correct operation and functions of the digital tachograph system represents one of the most serious threats to the security of the system. The use, or intention to use, such devices will distort fair competition, by giving unscrupulous operators and drivers an unfair commercial advantage; and create unacceptable negative social impacts for drivers by allowing, or forcing, them to drive for much longer periods than is legally permissible. The potential consequence of these factors is to undermine road safety, for all road users, and which the Commission is committed to improving over the coming years.

- 1.3. Furthermore, law-abiding operators and drivers must be able to trust the digital tachograph, and national control bodies throughout the Community must be able to rely on the authenticity and integrity of the data recorded and stored by the equipment, regardless of whether it is downloaded and analysed from the vehicle unit or the driver card. In order to guarantee the reliability of the data, regular checks and inspections of the equipment must be carried out to ensure its correct functioning and operation.

- 1.4. In the long-term, the total security of the system and its components is essential if the integrity and authenticity of the data recorded is to be assured. To bring to an end the most common abuses and attempts to defraud the system, the Commission will as appropriate examine the possibility of introducing further more detailed legislative measures in the review of Regulation (EEC) 3821/85 and its Annexes.
- 1.5. Nevertheless, in the short-term, appropriate and effective measures could be developed by the competent authorities of Member States in order to make the detection of manipulation devices much more likely, thereby reducing the risks that such equipment will be used by operators and drivers.
- 1.6. Whilst Member States have a legal responsibility to require that checks and inspections are performed in such a way as to ensure the effective implementation of the Community social legislation in road transport, such periodic checks cannot guarantee that devices will not be installed and used later, after checks have been completed. Experience has shown that such devices are far more likely to be found during roadside checks when the vehicle can be inspected more closely. The frequency and nature of these checks by Member States ought to be encouraged so as to significantly increase the deterrent factor by increasing the risk of detection of such devices.
- 1.7. Appendix 10 (Generic Security Targets) of Annex 1B of Regulation (EEC) 3821/85 sets out the scope of security enforcing functions needed to ensure the integrity of the digital tachograph system. The security objectives of, and the threats to, the whole system have to be addressed by a combination of technical solutions, through ITSEC approval, as well as through physical, personnel and procedural means, which are the responsibility of Member States and tachograph manufacturers to implement. It is the intention then, of this Commission Recommendation, to suggest to Member States the most effective procedures, based on both research and known best practice, to support those procedural and personal means.
- 1.8. However, this Commission Recommendation should not be regarded as replacing those technical solutions provided for by ITSEC ⁽¹⁾, and in fact, ideally, could easily be used in conjunction with, and support of, them.
- 1.9. The report provided by the Joint Research Centre ⁽²⁾ has set out the kinds of known and potential attacks to the security of the digital tachograph. Therefore, this report could be used by Member States as the basis of putting in place the necessary steps and actions to ensure that adequate information and guidance can be provided to the national control officers so that when they undertake checks and inspections of vehicles at the roadside, they can do so. Furthermore, similar information and guidance could be provided to fitters and workshops that carry out statutory installations, inspections, checks and repairs of recording equipment in road transport. The guidance could be of a sufficient scope to ensure that such persons can fully and competently carry out the checks described in this annex and that Member States are able to act in prosecuting those identified as abusing, or attempting to abuse, the system.
- 1.10. The following guidelines and recommendations are not exhaustive and there may be circumstances where the application of such recommendations cannot achieve the desired result (for example, in cases where the reference cable cannot be connected to the motion sensor). In such circumstances, Member States could be encouraged to develop alternative methods that can be verified as being as effective. Such alternative measures could be more widely shared amongst the enforcement community.
- 1.11. Furthermore, although this Commission Recommendation is intended to address both types of tachograph as defined by Regulation (EEC) 3821/85 and its Annexes, Member States may have methods, procedures and guidelines already established concerning checks of Analogue tachographs and the detection of manipulation devices. Therefore, this Commission Recommendation should not be seen to replace or detract from those measures already established, but to further support them, in particular with reference to the digital tachograph, where the methodology may differ, but the objective remains the same. It is recommended that where measures are already in place for checking analogue tachographs, they could, where appropriate, be extended to include digital ones also (for example, situations concerning the payment to workshops for carrying out specific tasks designated to them by control officers having directed a vehicle to an authorised workshop, as described in Section F).
- 1.12. Member States should be confident and supported in setting out in their national enforcement strategies their methods and processes in addressing the developing threats to the tachograph system. Such best practice could be shared with other Member States.

⁽¹⁾ ITSEC – Information Technology Security Evaluation Criteria, 1991 Version 1.2.

⁽²⁾ JRC Technical Notes. 'Report on the attacks to security of the digital tachograph and on the risk associated with the introduction of adaptors to be fitted into light vehicles'. Limited circulation to national risk managers (29 November 2007).

Chapter 2: Effective roadside checks

A. Organisation and equipment

- 2.1. In order to carry out full and effective checks, control officers should be fully equipped and properly trained. They should at least be in possession of control cards and have the relevant tools to download data files of the vehicle unit and the driver card and to be able to analyse such data files and print-outs from Annex IB type recording equipment in combination with sheets or charts from Annex 1 types. Control officers should also be equipped with software which has the capacity to analyse such data speedily and with the least inconvenience, since it is recognized that, for the purpose of detecting manipulation devices, print-outs cannot easily be analyzed at the roadside given the length and content of some of the files to be printed.
- 2.2. As far as possible, when control officers carry out checks, whether at the roadside or at the premises of undertaking, and whether dedicated to checking drivers hours' compliance, or roadworthiness tests or other kinds of checks, they could also take the opportunity that the time presents to test the correct functioning and use of the tachograph, and be able to detect the use of manipulation devices from such checks.
- 2.3. To this end, it is recommended that Member States attempt to organise checks of vehicles for manipulation devices, in conjunction with other checks (such as roadworthiness tests, conformity of Drivers' Hours Rules, etc) and that, indicatively, at least 10 % of the total number of vehicles checked are checked for the presence of manipulation devices. It remains for Member States to determine the appropriate methodology and circumstances for performing such additional checks, but the content could be reflected in their overall national enforcement strategy.
- 2.4. Effective checking could be undertaken using, for example, the following methods:
 - double check points with analysis of speed or distance (see B);
 - single check point with detailed analysis of data (see C);
 - single check point based on technical control (see D).
- 2.5. If a control officer believes that he has collected enough evidence, he could direct the vehicle to a workshop to perform further tests (see E).
- 2.6. Of course, additional, or alternative, methods of checking vehicles can always be deployed by Member States.

B. Double check points methods with analysis of real speed and distance of vehicles

- 2.7. Speed control at a specific time: to apply this method, control officers, using fixed or mobile cameras, or speed-guns, could measure real speed of the vehicle before stopping it at the roadside check at a specific time. They could then download from the Vehicle Unit (VU) the *24-Hour Detailed Speed File* and compare the speed recorded at this specific time with the one measured few kilometers before. At the checkpoint, this method only requires to compare two figures after having downloaded the *24-Hour Detailed Speed File*;
- 2.8. Fixed distance control at a specific time: to apply this method, the checkpoint could be chosen at a known distance from a specific location where control officers have facilities or means to note the time when an identified vehicle has stopped or crossed this specific point (toll tickets, camera records, reports of border controls, etc). At the checkpoint, the enforcers could then download from the vehicle unit the *24-Hour detailed Speed File* and compare quickly the average speed recorded between the checkpoint and the specific location with the one calculated from the known distance out of the time needed to reach the checkpoint.
- 2.9. With both methods, enforcers at the checkpoint need only to compare two figures after having downloaded the *24-Hour Detailed Speed File* and measured or calculated the real average speed. Any significant difference could give rise to a control officer having a suspicion that a device was used. The control officer could then direct the driver and vehicle to a workshop without necessarily having to perform further checks on the spot.
- 2.10. Concerning data from Annex IB type tachographs, all files that are downloaded from or through the recording equipment have to be accompanied by the appropriate digital signature that was originally generated by the vehicle unit or the driver card in order to verify the authenticity and integrity of the data and control officers could also check that this information is also downloaded.

C. *Single check point methods based on detailed analysis of downloaded data*

- 2.11. If a manipulation device is in use when a roadside check is carried out, or was in use until shortly before the check, indications of manipulation could be found through a number of simple procedures.
- 2.12. In order to establish the suspicion of the presence of a manipulation device, that would justify control officers taking whatever action they deem necessary to detect it, control officers could:
- Compare the driver's activities downloaded from the card and the vehicle unit with any other paperwork in the vehicle and driver's statements. Inconsistency between these data could constitute the beginning of a suspicion. In that case, the enforcer could investigate further.
 - Examine the *Events & Faults File* stored on the vehicle unit, and especially for the last 10 days:
 - Security breach attempt;
 - Power supply interruption (the longest event);
 - And Motion data error (the longest event);
 - Sensor fault.
- If the driver is not able to explain and justify the rational of each events or faults, the enforcer could investigate further.
- Examine *Technical Data Files* stored on the vehicle unit, and especially:
 - Time adjustment data.
 - Calibration data (five most recent calibrations, name of workshop and their card number).
 - The later data are useful to detect too many calibration actions that may imply that they have been performed with a stolen workshop card (or of a workshops card reported as lost). It is recommended that control officers check with their Card Issuing Authority ⁽¹⁾ the status of such workshop cards that have been identified, and whether they were valid at the time they were used to calibrate the vehicle unit.
- 2.13. If, after examining all the data mentioned in 2.14- 2.19, the control officer still considers that something is wrong, he could download the *24-Hour Detailed Speed File* and check, still with the help of his software, if there are unrealistic increases or decreases in acceleration of the vehicle and, where appropriate, if the profile of the journey is consistent with other paperwork in the vehicle and driver's statements (number of stops, speed in mountain or urban region ...). This evidence cumulated with the former ones could justify grounds to suspect that a manipulation device is present.
- 2.14. At the checkpoint, this method requires appropriate software, able to generate a readable display of the time profile of the speed in order to pin-point unusual variations in acceleration or decelerations of speed to highlight, and more generally to automatically signal:
- the unrealistic increases or decreases in acceleration of the vehicle;
 - any suspicious calibrations of the vehicle unit;
 - power supply interruption.

D. *Single check point methods based on technical control of seals*

- 2.15. Where possible, and when it is safe to do so, the control officer could check the seals. If the seals are absent, broken or damaged, the driver should be asked to justify the situation.

⁽¹⁾ TACHONET should be used to send request to other card issuing authorities.

- 2.16. If the driver is able to provide the written statement giving the reason for such action as foreseen in Chapter V section 4 of Annex 1, or requirement 253 of Annex IB to Regulation (EEC) 3821/85, then the control officer could require the driver to go to a workshop to reseal the system and recalibrate the equipment.
- 2.17. If not, this could constitute an infringement and it is recommended that the driver, with his vehicle, be directed immediately to an authorised workshop accompanied by the control officer for a check of the equipment as foreseen in the following chapter 3.

E. Directing the vehicle to a workshop

- 2.18. If after a roadside check using the previous methods, a reasonable suspicion still exists that a manipulation device is fitted, the control officer could direct the vehicle to an authorised workshop. Control officers, or the appropriate national authority, could be empowered to instruct authorised workshops to perform specific tests designed to test for the presence of manipulation devices.
- 2.19. These specific tests would allow, in most cases, the detection of the wrong pairing between the motion sensor and the vehicle unit, and which may indicate the presence of a manipulation device. Such tests could include (see description in Chapter 3):
- an inspection of the seals and the installation plaques;
 - a reference cable test;
 - an analysis of the downloaded data files.
- 2.20. If manipulation devices are detected, whether or not they have been used by the driver, the equipment (and this may including the device itself, the vehicle unit or its components, and the driver card) could be removed from the vehicle and be used as evidence.
- 2.21. Furthermore, authorized workshops could also be required additionally to check that the recording equipment: (a) works properly; (b) records and stores data correctly and; (c) that the calibration parameters are correct.
- 2.22. It is recommended that, for vehicles equipped with Annex IB type recording equipment, and only after downloading all data files and analyzing them (with their digital signatures in tact), and after checking that there is no manipulation device, that the recording equipment is fully re-calibrated and a new installation plaque affixed. Furthermore, it is recommended that only under the direction of the control body should the authorized workshop reseal the system.
- 2.23. Concerning recording equipment conforming to Annex 1, the equipment could, after the removal of any manipulation device, be checked for its proper functioning and correct operation, and be fully re-calibrated and a new installation plaque affixed. It is recommended that only under the direction of the control body should the authorized workshop then reseal the system.

F. Checking vehicles or data at company premises

- 2.24. It is recommended that Member State Competent Authorities take advantage of the possibility to check vehicles (and vehicle units) and drivers (and driver cards) which may be on site during a check of the premises of the undertaking.
- 2.25. Data managed by the undertaking is required to be kept for at least one year and made available for inspection whenever a control officer requests it. Therefore, as part of their standard checking procedure, control officers could check any vehicle that they find at the premises of undertaking, and to carry out whatever tests or activities they deem appropriate, whilst, at the same time, keeping delays to drivers and vehicles to a minimum.
- 2.26. Such checks at company premises could also take into account the possibility that there may be a mix of vehicles and records relating to either Annex I or Annex 1B type recording equipment, and it would be appropriate that control officers be prepared and properly equipped for this eventuality.

SUMMARY BOX**PREVENTING ATTACKS AGAINST DIGITAL TACHOGRAPH CHECKS AT THE ROADSIDE OR AT THE PREMISES OF UNDERTAKING**

National enforcement strategies could be developed to promote effective enforcement checks and inspections of vehicles that maybe fitted with manipulation devices, either at the roadside or during checks of premises of undertakings.

Properly trained and equipped control officers would be able to rapidly access, download and analyse data from vehicle units and to carry out checks promptly, and to be able to carry out similar analysis of data electronically stored, or in combination with sheets, charts and print-outs.

Member States could develop strategies to ensure that, when vehicles are checked for the presence of manipulation devices, such vehicles could be checked with one of the following methods by 2010:

- double check points with analysis of real speed and distance;
- single check point with detailed analysis of data downloaded;
- single check point based on technical control of seals.

Indicatively, it could be that 10 % of vehicles controlled (whether through roadworthiness tests, Drivers' Hours compliance or other checks) could also be checked for the presence of manipulation devices, although it remains for Member States to develop the most effective means, to be defined in their strategies.

If enough evidence leading to reasonable suspicion has been found, control officers could direct the vehicle to an authorised workshop to perform further tests.

If manipulation devices are detected, whether or not they have been used by the driver, it is recommended that the equipment be removed from the vehicle and used as evidence, in compliance with national rules of procedure relating to the handling of such evidence. Control officers could apply the appropriate processes and penalties associated whenever the use of such equipment is established, since it constitutes a most serious infringement.

Chapter 3: Training, equipment and best practice

- 3.1. Whilst Member States should ensure that control officers are properly trained for the execution of their tasks, adequate training could also be undertaken for all other relevant parties; it would be advantageous and highly desirable if joint visits and co-ordination for control officers between Member States were organized to harmonize best practices and diffuse lessons learnt from experience amongst practitioners.
- 3.2. Control officers should be adequately equipped in order to carry out the range of checks related to the digital tachograph. This means that they should have that the appropriate tools available to them to read, print and download data from such recording equipment. Member States could make efforts to ensure that a sufficient number of their control officers are thus equipped.
- 3.3. Best practice for detection and prevention, both during roadside checks and at the premises of undertaking (such as the use of the reference cable, the fixed-distance technique, detection of abnormal speed traces or distance profiles, breaks in power-supply, broken seals) could be shared and promoted within the enforcement community.

Chapter 4: Workshop inspections

Workshops and fitters provide a crucial link in the security of the tachograph system, irrespective of whether the equipment is an analogue or digital tachograph. Their approval and authorisation must be based on a clear set of national criteria which establishes their reliability and trustworthiness. To this end it is recommended that Member State ensure that workshops authorised to install, activate, calibrate, inspect and repair recording equipment are approved, regularly controlled, certified and provided with timely, relevant updates and information. It is also recommended that Competent Authorities provide fitters and workshops with clear instructions and guidance about their duties and responsibilities, in particular their understanding of their role within the context of the overall security of the system. It is also recommended that those authorities who approve workshops and fitters provide, through the Commission, to all other Member States, accurate and regularly updated information concerning the markings of seals and details and status of each workshop on their territory.

A. Legal basis

- 4.1. Vehicles will normally be required to go to a workshop for inspection whenever:
 - (a) the tachograph requires its inspection in compliance with the Annexes of Regulation (EEC) 3821/85;
 - (b) the vehicle undergoes its annual roadworthiness inspection under the provisions of Annex II of Directive 96/96/EC;
 - (c) control officers direct the vehicle to a workshop in order to carry out a more detailed inspection of the recording equipment;
 - (d) the recording equipment needs to be repaired or replaced.
- 4.2. On all these occasions, workshops or fitters could be instructed to visually and physically check that the recording equipment is sealed and that the recording equipment has both its manufacturer's descriptive plaque and the installation plaque.
- 4.3. Workshops could be regularly reminded by their Member State Competent Authority that whenever they inspect and reseal the tachograph system, and affix an installation plaque, then the workshop is, effectively, confirming that the system is secure, that it functions correctly, records properly and that there are no manipulation devices attached to the equipment.
- 4.4. Workshops could be reminded that they may be committing a serious infringement if they knowingly reseal the tachograph system without first removing any manipulation device that they themselves find, or requesting that the manipulation device is removed prior to resealing. If it is later established that a manipulation device is present, irrespective of whether it has been used or not, and that the workshop did reseal the system, and affix an installation plaque, then the workshop and individual fitters could be held liable of a serious infringement.
- 4.5. It is recommended that, given the important role that workshops and fitters have with regards to the security of the system, that Member State Competent Authorities consider appropriate sanctions which may even lead to the loss of approval or the authority to carry out work on tachographs, if workshops cannot be any longer relied upon.
- 4.6. Conversely, Member States could remind workshops that they have the right to refuse to carry out any further inspections or calibrations on any vehicle if they suspect, or know, that a manipulation device is present on that vehicle. Workshops could be supported by the Competent Authority if the workshop insists that, before continuing with an inspection, the manipulation device is first removed. The workshop can always refuse to either reseal the interface connections, or affix any installation plaque until the device is removed.
- 4.7. Those Member States which consider it appropriate could request that authorised workshops report such facts as described in 4.4 – 4.6.
- 4.8. Alternatively, Member States who do not consider such action by the workshop as appropriate could instead instruct workshops that such reports be kept for a specific period of time and made available to the Competent Authority when requested. This period of time could be a minimum of 24 months which would be in line with the minimum period between inspections of the equipment.
- 4.9. Workshops could also be reminded that simply removing a manipulation device from a vehicle does not necessarily exonerate the operator or driver from any infringements, since it is very likely that data previously recorded and stored on the vehicle unit and individual driver cards may have already been manipulated. By not reporting the matter, workshops could themselves be contributing to any offences committed by those operators or drivers and could expect to face the same punishments if caught.
- 4.10. Nevertheless, workshops and fitters could report the use or presence of manipulation devices to their Competent Authority who, in turn, could, for example, consider reward or incentive schemes to encourage workshops to provide information contributing to the detection and prevention of manipulation devices or any other types of attacks to the system.
- 4.11. The following guidelines and recommendations are not exhaustive and there could be circumstances where the application of such recommendations cannot achieve the desired result (for example, in cases where the reference cable (section 1.23) cannot be connected to the motion sensor). In such circumstances, Member States could develop alternative methods that are as effective. Such alternative measures could be shared amongst the wider enforcement community.

4.12. Furthermore, since these guidelines cover both types of tachograph as defined by Regulation (EEC) 3821/85 and its Annexes, Member States may have methods, procedures and guidelines already established concerning checks of analogue tachographs and the detection of manipulation devices. The guidelines in this Commission Recommendation should not, therefore, be seen to replace or detract from those measures already established, but to further support them, in particular with reference to the digital tachograph, where the methodology may differ, but the objective remains the same. It is recommended that where measures are already in place for checking analogue tachographs, they could, where appropriate, be extended to include digital ones also. For example, situations concerning the payment to workshops for carrying out specific tasks designated to them by control officers having directed a vehicle to an authorised workshop.

B. Broken or absence of seals

- 4.13. Workshops can always check if the seals are absent, broken or damaged.
- 4.14. Under no circumstances should the vehicle be resealed or issued with an installation plaque until the system has been restored to meet the requirements of the Regulation.
- 4.15. Workshops could record the fact that seals are missing on the inspection report or register and perform further checks (such as the reference cable check) and inspections to ensure that no manipulation device is present on the vehicle.
- 4.16. If, as foreseen in Chapter V(4) of Annex I, and Requirement 252 of Annex IB to Regulation (EEC) 3821/85, the seals have been removed in case of emergency or to install or repair a speed limitation device, then on each occasion seals being broken, a written statement giving the reason for such action has to be prepared and made available to the competent authority.
- 4.17. If not, the workshop could perform a complete check, with the following recommended methods and report to its Competent Authority precisely what has been done and detected.

C. Analysis of data records

- 4.18. Specifically to the digital tachograph, the data that could be downloaded, with its digital signature whenever possible, at the workshop and incorporated into the audit report should match the requirements contained in section 4.4 (Motion Sensor Security Targets) and section 4.4 (Vehicle Unit Security Targets) of Appendix 10 of Annex IB of Regulation (EEC) 3821/85. Appendix 1 provides the full list of the information in the audit report.
- 4.19. The workshop could also download and analyze the *Events & Faults Data File*, contained on the vehicle unit. These events and faults include for example (see also the full list in Appendix 2):
- security breach attempt;
 - motion sensor authentication failure;
 - unauthorized change of motion sensor;
 - unauthorized case opening;
 - power supply interruption event;
 - or sensor fault.
- 4.20. Detecting the use of a manipulation device after it has been uninstalled is also difficult to establish. However, a check of the *Events & Faults Data File* could show occasions when there have been power supply interruptions, which cannot be explained. Additionally, a study of the detailed speed trace could indicate abnormalities of the speed signal. Unrealistic decelerations or accelerations could be symptomatic of switching on or off a manipulation device.
- 4.21. In all circumstances workshops could print and attach the print-out to the inspection report or register (see Chapter 4) and, where appropriate, refer to any data downloaded using the workshop card.

- 4.22. If data from the vehicle unit cannot be downloaded using the workshop card, the vehicle unit may be considered as malfunctioning or broken. In such cases workshops could attempt to repair the equipment. If such attempts at repair still do not make it possible to download data, an undownloadability certificate should be issued, and a copy retained with the inspection report.
- 4.23. It is also recommended that drivers keep with them any undownloadability certificate issued to them by a workshop, in the event that they are later controlled when using a vehicle with a malfunctioning digital tachograph. It is furthermore recommended that, if the driver changes vehicles, then such certificates remain with the vehicle until such time as the transport undertaking can take receipt of the certificate as part of his overall record-keeping obligations and can have the equipment repaired.

D. Control of the pairing between the motion sensor and the vehicle unit

- 4.24. If any of the data described in the previous section is found to have occurred since the last inspection, the workshop could make a comparison between the motion sensor identification data of the motion sensor plugged into the gearbox with that of the paired motion sensor registered in the vehicle unit.
- 4.25. The use of a reference cable is an effective means of testing whether certain types of manipulation device have been installed into the vehicle. The reference cable is plugged into the back of the vehicle unit, and the other end connected to the motion sensor. If the motion sensor in the gear-box has not been paired with the vehicle unit, a 'motion data error event' or sensor fault will be triggered. This message will indicate the presence of a manipulation device. Should this event appear, the vehicle could be checked for hidden devices.
- 4.26. Alternatively, in the course of a check, the motion sensor could be unplugged and removed. If the digital tachograph system has not been tampered with, an error message will appear (no motion sensor). If, however, there is not such an error message, this will indicate the presence of another, concealed motion sensor or some other electronic manipulation device.
- 4.27. It should be noted that prior to using the reference cable technique, workshop technicians (or control officers) must insert their workshop card (or control card) in order to provide an explanation as to why the 'power supply interruption event' has been triggered and recorded on the *Events & Faults file* of the vehicle unit. Not to do so may give a wrong indication in the course of a later inspection that either the driver or operator may have attempted an attack on the security of the motion sensor.
- 4.28. Alternatively, although not always possible, the markings on the motion sensor on the gearbox could be compared with the motion sensor identification data of the paired motion sensor registered in the vehicle unit. Workshops could therefore carry out the following actions:

- A comparison of the information recorded on the installation plaque with the information contained within the vehicle unit record. Where it is found that information does not match, the Member State Enforcement Authorities could be informed and the incident recorded on the inspection report and the inspection register.
- A comparison of the motion sensor identification number printed on the body of the motion sensor with the information contained within the vehicle unit record. If needs be an electronic test tool could be used to check the electronic identification of the motion sensor. Where there is any mismatch of the identification numbers it can be assumed that a manipulation device is fitted. The Member State Enforcement Authorities could be informed and the incident recorded on the inspection report and the inspection register.

E. Special procedures as a result of a roadside check

- 4.29. Control Officers could have directed a suspicious vehicle to a workshop. In such circumstances, the control officers could firstly instruct workshops and fitters to download all data files from the vehicle unit. These files include the *Overview File*, the *Detailed Speed File*, the *Technical File* and the *Events & Faults File*. The appropriate digital signature must accompany such files.
- 4.30. A full check could be performed on the recorded data as well as with technical means (reference cable, check of the seals ...).
- 4.31. If serious inconsistencies are found but without the detection of a manipulation device, it could be concluded that a manipulation device has been used and removed. In such a case, the control officer ought to inform the body for the coordination of enforcement actions, according to Article 2 of Directive 2006/22/EC and/or the body for intra-community liaison, according to Art 7 of the same Directive, if the vehicle is registered in another Member State. This could lead to further investigation as far as the vehicle of the undertaking are concerned.

Chapter 5: Report and audit of workshops

- 5.1. Workshops could draw up an inspection report for each inspection of one vehicle where recording equipment is required to be inspected, whether the inspection is part of a periodic inspection, or at the specific request of the national competent authority. They could also record in a register the list of all the inspection reports.
- 5.2. The inspection report could be kept by the workshop for a minimum period of two years from the time the report was made and, whenever requested to do so by the national competent authority, make available all records of inspections and calibrations for that period.
- 5.3. Such findings made by authorised workshops, (records of broken, damaged or missing seals; missing plaques; incomplete or mismatched information between what was recorded on the vehicle unit and what was contained on the motion-sensor and; any detection of manipulation devices; copies of print-outs relating to the *Events & Faults File* and any other relevant print-outs), could, for example, form part of the regular reporting format and Member State Competent Authorities are encouraged to ensure that this is in fact the case.
- 5.4. Member States could consider that failure by workshops to provide duly completed inspection reports as a breach of the rules which may lead to the withdrawal of the workshop authorization.
- 5.5. Member States could perform audits of workshop inspection reports and registers at least once every two years. Such audits could include a random check of inspection reports related to the inspection and calibration of digital tachographs. Workshop cards could also be checked, and regularly downloaded to avoid data being lost or overwritten.

SUMMARY BOX

PREVENTING ATTACKS AGAINST DIGITAL TACHOGRAPH DURING WORKSHOP INSPECTION

When approving and regularly controlling workshops, Member States should ensure that their staff is properly trained and that they have access to all the necessary equipment to download data and carry out certain specific tests.

Workshops could be instructed by their Competent Authority not reseal a digital tachograph where a manipulation device has been detected until the device has been removed, and the tachograph fully recalibrated so that it records correctly. Furthermore, workshops could also be instructed by their Competent Authority to remove the installation plaque.

The inspections by workshops could include:

- physical checks of the seals, installation and manufacturer's plaques
- an analysis of downloaded data files, especially the *Events & Faults File*
- where appropriate a test with a reference cable technique

The workshops could record in an inspection report missing or damaged seals and attach to the report print-out of the downloaded files. The inspection reports could be made accessible to national authorities for two years.

The regular controls of workshops by Member States could include an audit of the inspection procedures, including a random check of inspection reports.

Member States could make sure that workshops inform the competent authority whenever they detect manipulation devices or find serious inconsistencies suggesting that a manipulation device have been used before to be uninstalled.

In such a case and when the vehicle is registered in another Member State, Member States could inform the body for intra-community liaison, in order to proceed with further investigation as far as the vehicle of the undertaking are concerned.

Chapter 6: Final provisions

- 6.1. Detecting and preventing the use of devices to defraud the tachograph system is an ongoing process and one that requires constant vigilance in addressing. As technology advances, so then do the methods and threats created to defeat the system. To this end all those involved in the security of the tachograph system, whether they are control officers, approved workshops and fitters, or legitimate and law-abiding operators and drivers, have a part to play.
 - 6.2. At national level Member States should be encouraged to obtain as much information as they can, to develop their own strategies in dealing with such threats, and strongly supported in the sharing of such information. New, or different threats, or attempts to defraud the system should be brought to the Commission's attention.
 - 6.3. At Community level, the Commission will continue to review the situation, and the application of the rules, and seek the support and co-operation of all Member States and industry stakeholders.
-