



Annex A to FESTA Handbook

Version 5

Legal and ethical issues in the execution of FOTs –
Worked Example

FOT-Net

(Field Operational Tests Networking and Methodology Promotion)

Legal and ethical issues in the execution of FOTs – Worked Example

The aim of this Annex is to sensitise the reader to the legal issues that will prove to be relevant in planning and carrying out a Field Operational Test (FOT). Due to the fact that the details of future field tests cannot be foreseen, all obviously relevant legal areas are covered; necessarily giving abstract information devoid of any warranty as far as completeness and accuracy for the concrete test arrangement is concerned. Considering the legal importance of details in test arrangements, it must be pointed out that it is vital to involve legal expertise from the country in question when planning a Field Operational Test. The overview given here can, furthermore, not substitute legal advice in a particular case.

1 Legal definition of “Field Operational Test”

Before the legal issues related with FOTs are discussed in detail, it must be defined that for the purpose of this section on legal and ethical issues, FOT is considered to be a test arrangement that is accomplished within real-life traffic conditions. This implies that an unknown number of persons not involved in the actual testing procedure, form the surrounding traffic. Usually third parties will not even know about testing being performed. Thus this first characteristic feature excludes artificial, isolated test arrangements and has important legal implications over all legal issues in question.

2 Information for test persons (briefing) / contractual agreements

The legal relationship between the organisation carrying out the field test and the test person will most likely have to be agreed upon in a contract.

A further characteristic feature of field operational testing is the data acquisition. In some way the driving will be recorded, possibly even the location might be tracked or videos of the driver and/or surrounding traffic recorded. This has an influence in terms of test persons' and third persons' data privacy and will partially be subject to consent on their side.

2.1 Preliminary considerations

To give substantial legal advice on exactly which information must be provided to test persons and estimate which arrangements (insurance, exceptional licenses, etc.) are necessary, rather detailed knowledge on the experimental setup and the systems to be evaluated is required. In order to conclude a contract with test persons, very detailed knowledge on the exact test design and testing procedure is necessary (and this at an early stage of the FOT).

As certain legal consequences may turn out to be unwanted, the following should be taken into account right from the beginning in order to adjust the design of the FOT accordingly.

2.2 Information provided to test persons

In order to obtain a valid consent from the driver to log the data and allow for safe participation in the FOT, information on the testing procedure and setup must be comprehensive. This does not include any technical knowledge about the layout itself, but all the consequences for the user: This will make the provision of information necessary on which kind of data is being logged in the first place and who will have access (esp. in case of accidents, administrative fines, etc. this will be important (see sections A.2.3; A.3; A.4.4; A.4.6). Possible legal consequences in case of dangerous driving by the test person should be specified (like possible recourse in case of grossly negligent or intentional behaviour – if applicable (and considered appropriate)). Special attention must be paid towards boundaries and how to deal with malfunctions (the two must be distinguished, see sections A.2.2; A.2.3). The same must be considered in case of a possible overload of the driver in terms of information, warnings, etc. That the responsibility for safe use as for administrative fines remains with the driver must be pointed out explicitly (see section A.3) as must be the fact that the driver remains fully responsible for his/ her driving and is not exempt from full responsibility due to participation in the FOT (this may not fully be applicable in case of non-overrideable systems, however, this will lead to many further questions, see section A.6.2). (Regan, 2006, volume 2)

Apart from this, the effect of the systems on driving – especially in case of some kind of unusual interference – should be pointed out, too. (This might be the case e.g. when applying a visual, acoustic or haptic warning-strategy that might unsettle the driver. (Regan, 2006, volume 2) Special information is particularly advisable in case of any interference into steering or braking, etc.). The risk here is to not sufficiently prepare the test person for safe use of the system. This may under certain conditions lead to liability of the responsible research scientist/ head of department and possibly to liability of the organisation (if possible according to national tort law). Apart from this, a researcher (even negligently) causing damage to the health of a test person may be considered criminally liable for unsafe test design, insufficient instructions and many further substantial breaches of his responsibility with obviously negative connotations for safety.

As a rule of thumb, about the same information and warnings, etc. should therefore be provided that would be necessary in a driver's manual, in case the system is meant to be used under real-life traffic conditions without further surveillance. Thereby, reasonably foreseeable misuse must be taken into account. The information should be provided in a way that the least informed test-person, who is therefore most exposed to a danger, can drive safely. The provision of information and warnings can, however, be achieved otherwise than in a written manual: Personal briefing, presentations on how to handle a system under certain conditions or the training of drivers with the possibility to experience the functioning and ask questions are legally sufficient as well. The possibility to ask questions at any time later during the FOT should be provided for e.g. by means of a telephone hotline (again in order to avoid insufficient briefing which may result in unsafe use by test persons). Furthermore, it might ex post turn out to be difficult to prove that a certain piece of information (that would have been necessary to avoid an accident) has actually been provided to the respective test person. Therefore it seems advisable to incorporate at least the most important information into the contract with a test person in form of some kind of notice or to refer to another document that has made the information available (see Regan, 2006, volume 2).

2.3 Information on system boundaries

A special issue in the context of briefing is system boundaries. System boundaries are those features of a system that are not a defect but still lead to wrong information or an erroneous intervention due to a lack of overall system intelligence (for further details and examples, see Deliverable D6.3).

As system boundaries always occur in certain situations, they are predictable and will not bring about liability issues as long as they have sufficiently been made clear to the test person. A test person who is able to anticipate the system behaviour in the case of all system boundaries will in this respect be considered well-informed.

2.4 Information on possible malfunctions

In case the FOT is taken out to evaluate a premature system, possible malfunctions will usually have to be taken into account too. Most important in case of malfunctions will again be to give test persons all the information necessary. That is first of all to provide the information, that a malfunction can occur and instruct thoroughly how to deal with the resulting situations (Regan, 2006, volume 2). If technically feasible, recognisability of malfunctions should be made possible. In most cases it will be sufficient to provide for the possibility to switch off the system and thus ensure safety. Even this might not be necessary as long as the malfunction will not impair safe driving at all. In case of intervening systems, however, much depends on the period of time available for a reaction of the driver: If this is too short, safety will potentially be impaired by any (disturbing) intervention.

For details on possible malfunctions related to the respective systems' intervention or information concept, see Deliverable D6.3.

2.5 Information on data recording

As far as data privacy is concerned, details are provided in a separate section (see A.4). For the briefing of test persons it is important to point out the relevant issues for data processing as well as access rights (Regan, 2006, volume 2).

It is legally required that the driver knows which data is being logged. It should also be pointed out, which conclusions can be drawn from the data available and this should involve all imaginable data sources and their combination (including external sources that can be resorted to). The meaning of anonymisation and pseudonymisation as well as any other measures to achieve data privacy should be described too. In case de-personalisation of data is possible and intended, it must be pointed out at which point of data-handling this is realised.

Example a: Within an FOT, data on speed as well as location is recorded. It is possible to anonymise the data for scientific use. However, when logging the data in the car, it can naturally be traced back to the driver (even if personal information is not logged). In this case, anonymisation might come into effect as soon as the data is read into a database with many similar recordings so that traceability of the test person is barred. Traceability would also be barred, in case the advice in section A.4 is applied. However, the risks of

accessibility in spite of these measures (see section A.4.6) – e.g. until pseudonymisation has been realised – should be pointed out too (in order to avoid incomplete information).

The most important measure to comply with data privacy regulations will be to inform the test person thoroughly as far as data acquisition is concerned and (voluntarily!) gain his/her consent. This consent must – due to the considerable impairment of data privacy combined with FOTs– be stipulated in written form. For all further details and advice, see section A.5 in this handbook (and details in the related Deliverable D6.3).

2.6 Agreements on cost allocation and liabilities (including insurance issues)

Another important aspect in terms of contractual agreements is the allocation of costs as well as special agreements in terms of liability. Some aspects will most certainly be regarded appropriate; some might seem disadvantageous in light of volunteer recruitment for a FOT.

However, the possibilities in terms of contractual agreements are broad as long as true freedom of decision is ensured (and participation must be voluntary anyway).

Appropriate agreements within an FOT will e.g. presumably be agreements on the allocation of fuel costs that will be borne by the test person. It may furthermore be regarded adequate to agree on a certain sum per mileage for the use of the test vehicle (as long as the vehicle can be employed in everyday use). This again may be combined with other agreements – in case of long term testing – within a lease contract, etc. (Regan, 2006, volume 1).

Of great importance in so far will be the agreements concerning the presumably valuable equipment for data acquisition (and possibly the units installed for evaluation). Here agreements on liability might be necessary as might be a special insurance in order to avoid a financial strain on the test person (and solve this conflict pragmatically). Compare section A.5.

Special agreements will be necessary on data provision by the test persons. As this will mostly be personal data, it shall in so far be referred to section A.4. However, it should be noted that apart from all the agreements necessary in terms of data privacy itself, agreements will also be necessary on how often data shall be retrieved, how this shall take place and the whereabouts of e.g. vehicle return, possibly the demounting of data acquisition components or systems (in case the vehicle remains in the property of the test person). In the latter case special attention must also be paid to possible damages brought about by installation of the FOT-equipment and how these shall be dealt with (Regan, 2006, volume 2).

In case the vehicle does not belong to the property of the test person, special agreements might be necessary in order to assure that the car is not used for dangerous driving. This will be evident from the data retrieved and in severe cases an obligation to intervene might even be brought about as the knowledge on the side of the researcher is evident (and the participation in an FOT might even provoke dangerous driving depending on the test-persons character). Therefore an appropriate contractual obligation may be stipulated by

agreeing on immediate termination of testing, in case dangerous driving is observed (Regan, 2006, volume 2). However, it must be pointed out that this knowledge on dangerous driving usually belongs to the private sphere of the person concerned. In case this knowledge would e.g. be disclosed towards the employer, this would severely compromise the test person and must therefore be dealt with in compliance with the guidelines depicted below (see section A.4). Any disclosure to third parties must therefore – all the more – be refrained from.

Another important aspect in terms of liability of the researcher is to ensure that the test-person is fit to participate in the FOT. This will definitely not imply any detailed inquiries as far as health is concerned (and this would even be considered intimate knowledge in terms of data privacy). Yet, the researcher should not allow a test person to participate in case an unfavorable medical condition is obvious. Apart from this, it might be a good idea to enlighten the need of good health in the FOT -information provided (especially e.g. as far as eyesight is concerned) and this might also be included in the contract dealing with all the details of FOT-participation. The same is true for any substance abuse (see Regan, 2006, volume 1).

Furthermore, information should be provided on the insurances concluded for the test vehicle (in order to point out remaining risks). Depending on the FOT model chosen, this might, of course, only be a recommendation to the test person on which insurances should be concluded (and may even be left completely to the test person in case the systems to be evaluated are mature, in no way critical and the test person owns the vehicle participating in the FOT). Special attention must be paid towards the insurance of data-logging equipment and special agreements might have to be made/ insurance issues pointed out to provide for sufficient information (see section A.5.3).

3 Administrative fines

In Germany, administrative fines are related to the personal responsibility of the perpetrator. If traditional driving is considered, no doubts exist on whether responsibility for any breach of traffic law remains with the vehicle driver. However, even systems that only provide information to the driver, tend to point out that traffic rules and traffic signs are prior to information provided (e.g. navigation systems). Therefore the following possibilities for system-design must be considered separately:

3.1 Informing Systems

As far as informing systems are concerned, two different types of information must be distinguished: First of all, information may be (more or less) legally irrelevant (e.g. a system providing information on present fuel consumption). Often, especially in case of safety-relevant ADAS, the information will, however, be legally relevant after all. Here again it must be distinguished: On the one hand there is information e.g. on legal speed limits, sign-posted dangerous bends or information provided by road traffic codes. This kind of information has a direct legal implication as it is directly linked to the provisions of road traffic and thus to the conduct legally required. On the other hand, the information that lacks this direct link may become legally important e.g. in terms of a compensation for damages. The latter is, however, much subject to the contractual agreement and information provided to the test person (for further information on this, see section A.2).

As far as those informing systems are concerned that have been circumscribed to be directly linked to the provisions of road traffic, the question might arise, whether false information provided by the system will excuse or charge (as the case may be) the driver in terms of an administrative fine.

Example A.4.1a: The driver negligently misses a sign-posted speed limit of 50 km per hour at the road side. His car is equipped with a speed alert system so he checks the speed limit displayed there. For some reason the information provided is, however, wrong, a speed limit of 70 km per hour is displayed. The driver relies on the information of his system and drives at 70 km per hour. The driver is fined for speeding.

In terms of administrative fines, it does not matter how the driver has been instructed (at least, if the driver has been aware of the fact that he must generally comply with traffic rules when taking part in the FOT – this information must be provided to the test person, see Section A.2). In example A.4.1a it can be expected from the driver to adhere to traffic signs: Only traffic codes and sign-posted traffic information are legally relevant (no in-vehicle-applications have been introduced in a legally relevant way so far). Because the driver misses the sign-posted speed limit negligently, he can be charged for speeding. All the other information (such as the display of the speed alert system) has no legal implication (it is only a factual “add-on”-information). So even though the driver in example A.4.1a only relies on the wrong information displayed, this will not excuse him legally in a way that the fine cannot be imposed on him (ALBRECHT, 2005).

Example A.4.1b: The driver is speeding and is additionally warned by a speed alert system that he is going to fast. Due to data collection in the car, the display and acoustical signal of the speed-limit warning is recorded. As a camera is also installed, it can be proved that the driver has noticed the warning provided on the display. The driver does, however, not reduce his speed and is fined.

In example A.4.1b the driver is – apart from the sign post or general traffic rule – additionally warned by the in-vehicle-application (such as a “speed alert” system) and has obviously been aware of the speed limit. Therefore his breach of traffic law might be considered intentional, which may have effect on the height/amount of the fine: In Germany e.g. it is generally assumed that speeding is a negligent act. In case intention can be proved – which would be promising given all the data recorded here – the fine will turn out to be higher (ALBRECHT, 2005). This problem is also dealt with in Section A.4 (data privacy issues) as far as data usage in terms of prosecution is concerned. In case it proves to be necessary to record this data, the test person concerned (driver) must at least be aware of the risk he/ she is running (which is again subject to the information provided by the organiser of the FOT).

3.2 Intervening, overrideable systems

As far as intervening, overrideable systems are concerned, most important is to point out that they must be actually overrideable in any case and at any time (otherwise see Section A.3.3). If they are overrideable, the driver is still fully responsible for every movement of his vehicle. Usually the intervention will either serve as a basis for information transmission (e.g. vibration of the steering wheel) or will simply intervene by carrying out (a part of the)

driving task automatically (e.g. an Adaptive Cruise Control). As far as the transmission of information is concerned, the same will apply in terms of fines (this has been discussed in section A.3.1, see above).

In case the driving task is partially carried out automatically, the system boundaries and functioning of the system must be made completely clear (to provide for full control over the vehicle) and it must be pointed out that the responsibility – even for the aspect of the driving task carried out by the system – remains with the driver. It is therefore necessary to override the system, if this is legally required (and this must, of course, be possible!). All this is subject to the information provided to the test person (see section A.2). As full control over the vehicle will then still be immediately available, administrative fines can be imposed on the driver in case of a negligent or intentional breach of traffic law.

3.3 Intervening, non-overrideable systems

In case of intervening, non-overrideable systems, it should for the means of this handbook briefly be pointed out that these are generally considered non-permissible and call for exceptional licenses and a specific insurance (see section A.6.2 and A.5.4).

Apart from this, the driver is no longer capable of (fully) putting his will into execution as far as the control over his vehicle is concerned. In so far as the administrative fine arises from an aspect that no longer belongs to the drivers' control, the breach can no longer be considered negligent or intentional. Therefore administrative fines can no longer be imposed on the driver. (ALBRECHT, 2005)

3.4 Cooperative Systems

In case of cooperative systems many aspects may come to effect that have been discussed above in the sub-sections A.3.1, A.3.2 and A.3.3. The respective effect a cooperative system has within the car and the information on the cooperative system provided to the driver will then be respectively valid here. In other words, the same will then apply to cooperative systems.

4 Data privacy

4.1 Introduction/ general comments/ minimum standard within the EU

Data privacy is in Germany based on basic (constitutional) human rights (for Germany: Art. 1 para. 1 and Art. 2 para. 1 of the "Grundgesetz"= German constitution). This right is termed "informational self-determination" ("informationelle Selbstbestimmung"). The Federal Constitutional Court of Germany characterises this basic right as the authority of the individual to decide on the disclosure and use of his/ her personal data. This is substantiated with the argument that who cannot overlook which personal information is available in certain fields of his/ her social environment and therefore cannot estimate the knowledge of contact persons, can be substantially hindered to exercise his personal freedom of free decision and planning. This should well circumscribe the scope of protection data privacy acts bring about. [BfD-INFO 1, 2002]

Within Europe, the minimum standard of data privacy (“data protection”) is stipulated by the EU Directive 95/46/EG. This directive was issued in 1995 to ensure data privacy of natural persons in the processing of personal data. The directive describes the minimum standard for data protection that must be guaranteed throughout the EU by national law (the directive itself is generally not directly exercisable). In Germany the directive led to some modifications of national data protection acts such as the “Bundesdatenschutzgesetz” (BDSG). [BfD-INFO 1, 2002], (ROSSNAGEL, 2003)

The extent of protection by data privacy acts in Germany is rather dense. If therefore the data protection principles valid for Germany can be applied to the design of an FOT, it is most likely that this will be sufficient in terms of data protection for other countries of the EU too. However, it must be pointed out that the following statements can only claim definite validity for FOTs in Germany. In case of doubt, it seems advisable to contact the national data protection officer (if applicable for the respective country) for further advice (the same applies in case of any specific questions). It must also be pointed out that the standard of data protection can turn out to be lower in other countries, should, however, not drop below the minimum standard described in the EU-directive mentioned above. This minimum standard must be complied with, especially when taking out an FOT within an EU research activity. The minimum standard within the EU directive has also been referred to as far as possible.

4.2 Legally relevant data and general measures to ensure data privacy

Data privacy regulations are generally based on basic human rights. Therefore the scope of relevant data is restricted to personal data. Personal data are particulars on personal or factual relations of a defined or definable person. In some European Countries (Austria, Luxembourg, Denmark) even legal bodies are covered by data protection rules, however, as far as of interest for FOTs, data privacy of the natural person is in question (see Sec. 3 BDSG, Art. 3 EU Directive 95/46/EG). For further examples see Deliverable D6.3.

Anonymization and pseudonymisation are measures to assure data privacy.

Anonymization is the de-personalisation (a modification) of personal data. The data can then not be traced back to the natural person. However, it must be kept in mind, that complete anonymity cannot be achieved, in case the data is so particular that it will apply to only one person. Whether a data set can be considered anonymous, may be dependent on the number of particulars, the available methodological and mathematical instruments as well as the availability of additional information allowing re-personalisation. Therefore, anonymity must be considered a relative term.

In case of pseudonymisation the name or other identification criteria of a person is modified and replaced by a pseudonym (usually a multi-digit number, nick-name or combination of numbers and letters, the so called “code”). This will considerably complicate the identification of the person behind a data-set. However, in contrast to anonymization the re-identification remains possible (and is not restricted to chance, mathematical or methodological instruments). With the help of the key that has been separated from the original data set – possibly a list linking the names to the code – re-identification can be achieved. The protection of privacy is much dependent on how well the separation of the

key and data-set is ensured. If the key is destroyed, the data would be considered anonymised. (ROSSNAGEL, 2003)

4.3 Sub-constitutional law and general principles

For Germany, the basic right of informational self-determination has been further developed in sub-constitutional law. Such are the federal law on data privacy (“Bundesdatenschutzgesetz (BDSG)”) as well as respective acts in every single federal state. Depending on the background of the organisation taking out the FOT (company (= private) or public authority) different measures are applied in terms of data privacy. For the means of this report, the description of legal framework will focus on the BDSG as this code is generally applicable in case of data privacy for private organisations (companies, etc.) and valid for all federal public bodies (does, however, not apply to the public bodies within the federal states which are large in number: For these the respective act in the respective federal state is applicable. The provisions tend to be very similar, though). [BfD-INFO 1, 2002]

As a rule of thumb, the provisions are, generally speaking, rather strict in case of data acquisition, processing and use by public bodies and more liberal in case of (private) companies. Speaking for Germany, this leads to the situation that only those private companies, institutions, etc. are subject to the federal law on data privacy that collect, process or use data by means of data processing equipment (automated or not). The use of personal data in any other way e.g. by private entities is not subject to the act in the first place. However, data processing equipment will be the rule for field operational testing, so data privacy restrictions will in so far be applicable.

The basic principle of data privacy provisions in Germany is that any form of data acquisition and processing is interdicted, if not subject to explicit authorization within the same act (or some regulation by special law). [BfD-INFO 1, 2002]

4.3.1 Consent of test persons

Based on the provision that data acquisition and processing is generally interdicted, the most important exception from this rule for FOTs is the consent of the person concerned (see Sec. 4 and 4a BDSG, Art. 7 and 10 EU Directive 95/46/EG). For any consent given in terms of data acquisition, processing or use, the person concerned must:

- make this statement in written form (if not certain circumstances make another form necessary)
- the consequences must be clarified (intended purpose of acquisition/ processing/ use), including the consequences, if consent is not given
- the consent must even be specially highlighted, if the consent to data acquisition/ processing/ use is issued together with other statements (consent to the use, etc. of data concerning health – which might be of interest for FOTs – will call for a special (separate) consent in this respect)
- consent must always be given voluntarily!

[BfD-INFO 1, 2002]

4.3.2 Principle of purpose limitation

Another important principle is purpose limitation (Sec. 14, 28, 29 BDSG; Art. 6 EU Directive 95/46/EG). This means that data may only be processed for the same purpose it has been collected for (or saved, in case prior acquisition is non-applicable).

However, the act comprises a number of exceptions to this rule. As far as relevant for an FOT, acquisition, processing and use of data is not limited to the same purpose in certain cases (see Sec. 14 BDSG valid for public administration and Sec. 28 BDSG for private bodies). [BfD-INFO 1, 2002] For details on these exceptions see Deliverable D6.3.

4.3.3 Data acquisition (extent and limitations)

The general principle for data acquisition is that data must be collected frankly from the person concerned (and not otherwise). As far as data acquisition is taken out by a public body, this is only possible to such an extent as necessary to fulfil the legitimate tasks (Sec. 4, 13, 28, 29 BDSG; Art. 5-7 EU Directive 95/46/EG). The relevant limitations for private entities in case of an FOT are in so far

- specified in the contract on which data acquisition is based
- restricted to explicit consent in case of intimate and very private data (such as racial and ethnical background, political opinion, religious and philosophical belief, health and sex life). Especially data on the health of a test person might be important for the FOT. The acquisition will most likely prove permissible again for the reason of research: Here data acquisition must meet the legal principle of proportionality (and therefore go conform to an evaluation of the higher and therefore more valuable legal right) (see Art. 8 EU Directive 95/46/EG).

Apart from this, data acquisition is also limited by the principle of data economy (Sec. 3a BDSG). This is to say that no more personal data shall be collected and saved than is really necessary to fulfil the purpose in question (i.e. any unnecessary data compilation shall be avoided). [BfD-INFO 1, 2002]

4.3.4 Technical and organisational measures

An important and rather costly aspect of data privacy is the technical and organisational standard that must be applied. Generally speaking, those measures are necessary that will guarantee the compliance with data privacy (see Art. 16, 17 EU Directive 95/46/EG; Sec. 9 BDSG; Sec. 10 BDSG calls for further technical measures but concerns the automatically generated release order and should not be applicable to an FOT). What this rather general description can imply, has been stipulated in an annexe to the German data privacy act. The effort needed to ensure data privacy in case of automatic processing and usage is dependent on the character: Intimate data is most strictly protected and forms the core area that may not be impaired at all (will seldom be relevant in case of FOTs), personal, private data is strongly protected and data with a relation to other people that is generally known, is the least critical. The character of the data in question indicates the effort to be applied in order to achieve reasonable care.

General measures to ensure data privacy on the technical and organisational level are described in detail in the Deliverable 6.3.

4.4 Data privacy in research activities

Research is in itself a basic right of constitutional weight – as is data privacy, see above. Therefore, an appreciation of both values must be carried out for the case in question.

Research is facilitated within data protection regulations such as Art. 6, 11 and 13 Directive 95/46/EG and sec. 40 BDSG.

The regulation in sec. 40 BDSG emphasises the principle of purpose limitation to the object of research and explicitly calls for an anonymization of data at the earliest possible stage. Until anonymization can be achieved, the characteristics of the person concerned must be saved separate from the particulars on personal or factual relations and must only be brought together in case this is required by the object of research. Any publication of personal data can only be admissible in case the person concerned gives his/ her consent (if relevant for FOTs in the first place).

However (for Germany), no right of professional discretion has been stipulated in the field of research activities (as existing e.g. concerning confidential medical communication of a medical practitioner). This has important implications within criminal law, see below section A46. This may be completely different in other countries of the EU as the Directive 95/46/EG gives sufficient leeway for a deviant regulation. (ROSSNAGEL, 2003)

In order to achieve data privacy for the test persons in spite of these regulations, it has been suggested [ROSSNAGEL, 2003] to deposit data necessary for re-identification (after having pseudonymised the data) with a bearer of secrets (such as lawyers). Such a bearer of secrets can refuse to release data he/ she is entrusted with. It has further been proposed to store the personal data with the (test) person concerned (ROSSNAGEL, 2003). This implies the risk, not to obtain the data, because the test person might finally decide on wanting not to disclose the personal data at all. However, for an FOT this is an option to be considered: As far as the data recorded is stored within the car e.g. by means of a SD-card etc. this would allow the test person to remove the personal data and take care of it by himself/ herself (until it is handed over to the organisation taking out the research activity). The personal data is thus fully placed at the disposal of the test person up to its voluntary release. The test person is, therefore, free to decide upon the further use or existence of the data (and has every right to destroy the data if he/ she pleases). This will avoid conflicts arising from data acquisition and balance the risks implied to a great extent. From a practical point of view it should technically be ensured that the storage medium is easily accessible and removable (and it should not be too expensive either, because the test-person would supposedly be required to come up for a replacement in case of the storage medium's destruction).

4.5 Video recording

Video surveillance might be of great importance for FOTs: Only knowledge from surveillance of the surrounding traffic as well as the driver can determine the impact of a system and/or reveal why a sudden driver action is necessary, etc.

The conflict arises from the high quality of video data that can be achieved by today's technical possibilities in video recording. Additional processing of this data will therefore often reveal the personal identity. Privacy measures and regulations on data privacy in these cases are existent, but they are difficult to handle, see below. The problem with video data is that it is usually impossible to anonymise or pseudonymise images or even videos. This is why this data is especially 'delicate' in terms of data privacy and comprises great dangers. As such must be considered the threat that video-data might be made publicly

accessible over the internet (which would be illegal, if the video contains personal data and the test person has not granted his/ her consent prior to this release). Such a video, however, would only then be of great interest, in case the driver or a third party behaves in a way that calls for voyeurism. As the harm to data privacy of the person concerned (and thus his/ her basic right of informational self-determination) can be tremendous, it must be considered reasonable to delete such a sequence entirely as soon as possible (which is as soon as respective knowledge on the existence of the sequence is available). Otherwise, measures must be taken to secure the data adequately (which would be challenging).

From a legal point of view, it must be differentiated between data acquisition outside the car (surrounding traffic) and data acquisition inside the car. This should apply to the technical requirements as well.

Generally speaking, it is advisable, according to the basic principles described above, to do without any video surveillance (in case this proves possible). And pure surveillance (without any recording) is always the less inculpatory measure. Therefore data acquisition by means of video recording should only be employed if indispensable. However, this will usually be the case with FOTs so the following statements will concentrate on necessary video recordings. (ROSSNAGEL, 2003), BfD-INFO 1, 2002]

4.5.1 Video recording of third parties

Video surveillance by means of optical-electronic devices (video surveillance) is only permissible according to the guidelines provided in Sec. 6b BDSG and is also considered critical within the Directive 95/46/EG (see Art. 33 Directive 95/46/EG that contains a revision clause to enhance data privacy in case of video and image surveillance). As far as Sec. 6b BDSG is concerned, it has been criticised that a differentiation of private (video-) data acquisition and video surveillance by public bodies is not made. The scope of sec. 6b BDSG therefore comprises public as well as private bodies and according to its wording it is only applicable to the “surveillance” of publicly accessible places (which would apply to roads).

This, however, does not lead to the conclusion that other recordings are irrelevant in terms of data privacy (this is only the case with really private recordings such as those taken within a family). Any (other) video recordings must therefore meet the provisions stipulated in sec. 6b BDSG, in order to achieve compliance in case of video-data acquisition by non-public institutions. Data acquisition must therefore comply with the following requirements:

Data acquisition must be taken out frankly. A hidden camera will therefore not be regarded permissible as long as consent of the persons concerned has not been obtained.

A legitimate interest for video-data acquisition must exist (see sec. 6 para. 1, No. 3 BDSG). In case of an FOT the concrete legitimate interest will be the same for which video data must be recorded in the first place (and cannot be done without). In case of research (a value of constitutional weight too, see above and Art. 5 para. 3 Grundgesetz = German constitution) the concrete legitimate interest is implicated by the motivation (research).

The video data must be necessary in order to achieve the purpose identified as the legitimate interest. Here it must be considered that the storage of data must also be

indispensable, as any storage of video data is considered ultima ratio. This should be overcome in case of an FOT, as long as there is sufficient need of video data.

The video data must be deleted as soon as it is no longer necessary in order to achieve the legitimate purpose of research, see sec. 6b para. 5 BDSG. The same will apply in case of a protection-worthy interest of a third party which is in conflict with further data storage.

(ROSSNAGEL, 2003), [BfD-INFO 1, 2002]

4.5.2 Video recording of the driver

The situation for the driver differs strongly. Basically, however, the same requirements and regulations are valid in this case. The main difference is that the driver will always have to give his/ her consent to the video recording as the permanent recording within the car is strongly invasive. By no means may the recording be taken out with a hidden camera and without informing the driver beforehand. (see ROSSNAGEL, 2003)

Further care must be taken not to record any video data of other passengers, if this can be avoided by technical means (as usually a legitimate interest in so far will not exist, and, as mentioned above, the principle of data economy must be applied). In case the video recording of other passengers is inevitable, it must be ensured that the camera is well on view and thus obvious that data is being recorded. The designated test persons must in this case further be sensitised to inform any passenger of the recording. The same will, of course, apply to any further drivers of the car. It may, however, for a number of reasons be a good idea to restrict the use of the participating vehicles to the actual test person or provide for a “switch off” of all systems and data logging (for safety and data privacy reasons) in case other drivers use the vehicle. This will not only provide for consistent data (which should be necessary from a scientific point of view) but at once ensure that all the contractual agreements actually reach the driver.

4.6 Implications of criminal law

If the FOT goes according to plan, criminal law will not be affected. However, in case of accidents, the data collected might be used otherwise. In this case, personal data of the test person will have been recorded to an extent that is generally not available in this situation in the first place. As the breach of certain traffic rules may be relevant under criminal law aspects, the data will be of interest for means of criminal prosecution as well. This, at least in case the availability of the data is known; however, due to possibly obvious modifications within the vehicles (perhaps even a camera is on view for video-recordings) further inquiries in this respect seem probable. It must therefore be expected that the data might even be subpoenaed on application of a public prosecutor by a judge. For Germany this possibility is given, see sec. 94 seqq. StPO (Strafprozessordnung = Code of criminal procedure). In this context it must be pointed out that these legal effects will be tolerated in Germany and the recording for research-reasons will not privilege the test-person (i.e. it would not be barred to confiscate the data for the reason of criminal prosecution). And data privacy provisions (for Germany) will not bar the use of this data for the reason of criminal prosecution either.

In case the data is already in hold of the organisation doing the research, it would have to be released anyhow (see sec. 95 StPO) – in spite of the fact that this might mean a moral

dilemma for the researcher involved in the FOT. These effects, however, may be largely avoided if the procedures suggested for the means of ‘data privacy in case of research activities’ (see section A.4.4) are taken into effect.

In this context, it must be pointed out that a suspected person always has the right to remain silent in order to avoid self-incrimination (i.e. the accused is not obliged to cooperate actively in the own conviction: “*nemo tenetur se ipsum accusare*”). It will therefore not be considered a criminal offense in itself, in case the accused would delete or destroy the data recorded. As far as a civil court, however, will decide on compensation for loss suffered, conclusions can be drawn from the fact that the data has been deleted/destroyed.

5 Insurance

5.1 Introduction

This section exemplarily goes into the legal situation for Germany as far as road traffic liability and the associated insurance issues are concerned. This should allow for sufficient insight in this aspect to sensitise for possible arrangements and precautions to be taken as far as the insurance of the test-vehicles is concerned.

5.2 Road traffic liabilities in Germany

According to national road traffic liability law in Germany, accident victims can potentially claim for compensation from the “keeper” of a vehicle (“Fahrzeughalter”, see below), the driver and the vehicle’s insurance.

The “keeper” of the vehicle will usually at once be the legal owner; however, this is not invariably true. From a legal point of view, the “keeper” is generally defined as the person that makes use of the vehicle at own expense, i.e. comes up for the costs and has the capitalised use (HENTSCHEL, 2007). The “keeper” will be liable for any damage to the legally protected interest resulting from the operational hazard. The only (basic) requirements for a claim in so far are that the vehicle was in use at the time the damage occurred (this, however, can even be assumed when parking in public space) and that the vehicle’s use (i.e. its operational hazard) has led to a damage of the legally protected interest. In case a further vehicle plays a part in the emergence of the damage to the legally protected interest, its respective contribution will be considered too. The same applies to contributory negligence of the damaged person. In so far this applies to the causation giving rise to the damage of the legally protected interest. In a further step the remoteness of further damages incurred that can be traced back to the damaging event are considered too.

Unlike the “keeper”, the driver will only be liable in case of fault (e.g. any driving mistake, etc. that leads to a damage of the protected interest). Apart from this, the driver is, generally speaking, liable for the same damages to legally protected interests as the “keeper”. If the driver’s and “keeper’s” liability is given, they will both be jointly and separately liable (together with the insurance, see below) for the damage (a term that describes that the damaged person can decide freely which debtor to claim against for the whole damage – which is then settled between the two or more debtors).

Of course, the damage the “keeper” as well as the driver are liable for, is insured via the same compulsory car insurance. By provisions of law the “keeper” is obliged to contract such an insurance in case he wishes to operate his vehicle on public roads. It is regulated that the contract covers the damage on account of the driver as well as the compensation for damages imposed on the “keeper” (and as long as the contractual obligations are adhered to, no recourse will be taken). In Germany, a direct claim of the aggrieved party against the insurance is admissible according to provisions of law. (ALBRECHT, 2005)

5.3 Insurances for road traffic in Germany

In so far as material damages are concerned, it is – according to the situation in Germany — important to distinguish between many different types of insurances. First of all, the compulsory road traffic insurance will cover the damage to the property or health of a third party (automobile third party insurance – as stated above, this insurance is compulsory in Germany and therefore widespread and generally referred to as the “car insurance”). It will, however, neither cover the physical damage to the “own” vehicle nor the damage to the health of the driver and other occupants. As far as the physical damage to the car is concerned, a special insurance can be obtained to cover this (comprehensive insurance/comprehensive coverage insurance including collision). As far as the health of occupants or other passengers is concerned, a special motor passenger personal accident insurance type exists that will come up for damages to passengers. However, it must be kept in mind that the insurance sum for this insurance is usually restricted (and will generally not be sufficient to adequately compensate for serious injuries, special medical care requirements, etc.). Furthermore, the driver might be excluded in this insurance – here a special insurance may prove necessary (driver personal accident insurance). This, however, is again usually limited to certain insurance sums that may not prove to be sufficient for full coverage. Therefore it may appear to be reasonable in some cases – according to the field test design chosen – to obtain some kind of special insurance tailored to the special needs of the specific field trial (e.g. clinical trials insurance).

Most important in all cases will be to disclose the fact towards the insurance that the vehicle is participating in an FOT (which in general should simply be accepted by the insurance). Insurance rates might rise, however, depending on the systems integrated in the vehicle (subject to the FOT, likely in case of premature systems which might involve additional risks). Disclosing this information and possibly incorporating a respective clause in the contract will be a reasonable method to avoid legal uncertainties as far as insurance coverage in case of an accident is concerned.

5.3.1 Automobile Third Party Insurance

As stated above, this insurance is compulsory by law. The minimum insurance sum for this insurance type is e.g. in Germany fixed for motor vehicles at 2.5 Million Euro in case of damages to health (in case of fatal injuries or more than three persons injured: 7.5 Million Euro) and in case of damage to property even limited to 500 000 Euro (see annexe 1 to Sec. 4 of the obligatory insurance law = “Pflichtversicherungsgesetz”). These, however, do not necessarily cover the whole damage in case of serious accidents and even the maximum compensation sums according to the German road traffic act (which is

below the minimum insurance sum) can be exceeded in case the claim is based on the law of torts (in this case a maximum compensation sum no longer exists).

It is therefore reasonable to raise the test persons' awareness to these (general) limitations (see section A.2.3) and, if considered necessary, the test vehicle should be insured to better conditions.

5.3.2 *Comprehensive insurance/ comprehensive coverage insurance including collision*

It must further be decided on the necessity of comprehensive coverage insurance. This insurance will replace the material damage to a vehicle even in case of self-inflicted accidents (depending on the contract). The insurance will usually exclude intentional damages and may exclude damages resulting from gross negligence. This insurance is not compulsory. If it is renounced, it must beforehand be decided and agreed upon who will come up for these material damages (this insurance would cover) in order to provide for legal certainty. Possibly this has influence on the information that should be provided to the test person, see section A.2.

5.3.3 *Motor passenger personal accident insurance*

In case of damage to the passengers, compensation can be obtained within the automobile third party insurance of the injuring party. In case of hit and run accidents, absence of insurance coverage of the third party, etc. compensation can be claimed from the personal accident insurance. It will cover all those damages to health involved from the time the passenger gets in the car until he gets out again (HIMMELREICH/HALM, 2006).

This personal motor passenger accident insurance will generally cover costs for medical treatment as well as the costs involved in the event of motor passengers' death.

This insurance shall not be enlarged on within this report. However, selected aspects shall be pointed out: This insurance will not necessarily cover the damage to the driver (which may, however, be the case). And insurance sums vary strongly. They may not be sufficient to cover severe health injuries or the costs involved in case of disability. Special attention must therefore be paid towards the maximum sums. Further information on this type of insurance should be gathered in the planning of the FOT (if applicable and considered necessary within the test design chosen). (HIMMELREICH/HALM, 2006). Driver Supplementary Insurance

The Driver Supplementary insurance (= "Fahrerzusatzversicherung") is a fairly new insurance type and is largely unknown. The conditions of insurance may differ strongly. Motor passengers are in Germany (since 1st Aug. 2002) covered by the Automobile Third Party Insurance. This is even the case, if it comes to a self-inflicted accident caused solely by the driver of the vehicle they are occupying. In this case, the passengers can claim for compensation against the vehicle's Third Party Insurance. Therefore today only very particular cases depicted above will leave passengers without insurance coverage.

The driver, however, is the only car occupant who may not be able to claim for damages (or only have a partial claim against the third party's insurance). This Driver Supplementary

Insurance will cover these damages as far as compensation cannot be obtained otherwise. This insurance type is generally considered reasonable. (HIMMELREICH/HALM, 2006).

5.3.4 Clinical Trials Insurance

As stated just above in this section, the risk of damage to the health of the driver (who is at once the test person) is severe and must be considered beforehand. Of course, the testing in open traffic will also involve many further risks to third parties which must nonetheless be considered. Therefore the justifiable risk will be limited strongly in the first place.

Shall a greater risk nonetheless be taken (and this be considered otherwise permissible), a clinical trials insurance may be necessary to cover the risks involved. As far as (medical) clinical trials are concerned, this insurance type is common. For the purpose of road traffic such an insurance would have to be tailored according to the specific needs of field operational testing.

5.3.5 Test Equipment Insurance

The data-logging equipment and possibly prototype systems may have to be insured too by means of property insurance. This should be kept in mind when planning a Field Operational Test. This electronic equipment will usually not be covered by the comprehensive insurance/ comprehensive coverage insurance including collision (as maximum insurance sums for common electronic equipment in vehicles will assumedly be exceeded by far).

5.4 Insurance issues in case of non-overrideable systems

A basic principle of European road traffic is driver's full control. Therefore non-overrideable systems that influence the driving task, comprise unsolved and complex legal questions that cannot be fully assessed at present (see "Communication from the Government of the Federal Republic of Germany to the European Commission of 27 June 2007" page 6, stipulating conclusions of the eSafety Conference in Berlin on 5th/6th June 2007).

As far as insurance issues are concerned, it must therefore be taken into consideration that any type of insurance known today assumes full driver's control. In case the Field Operational Test is otherwise regarded permissible (see section A.6 and A.7), special arrangements for specific insurance coverage must be taken into consideration.

5.5 Insurance issues in case of cooperative systems

Cooperative systems may comprise very specific insurance issues in case the influence on the driving task is strong: If the cooperative aspect therefore involves any kind of vehicle control, it must further be taken into consideration that all present regulations on road traffic are based on the assumption of a vehicles (and driver's) autonomy. In case control of a vehicle is therefore dependent on other vehicles (the same for road side beacons) it must be assessed whether common liabilities (and thus insurance contracts) will sufficiently cover all possible damages in between the linked ("cooperative") vehicles and towards surrounding traffic. If this is no longer the case, it might turn out to be a legally challenging task to tailor the insurance contract to fit the actual "cooperative" situation.

6 Vehicle licensing requirements

6.1 Licensing requirements for motor vehicles in general

As long as the Field Operational Test is focussed on the evaluation of applications already approved of as optional or standard fitting of the test vehicles, no vehicle licensing requirements will be in question.

The licensing of a vehicle for Europe is generally taken out by means of type approval according to technical rules and regulations in international law. For Europe the so called ECE-Regulations are binding (and their fulfilment will be considered sufficient for road admission throughout Europe). However, gaining a type approval certificate for a new vehicle type is challenging and costly and can hardly be considered an appropriate approach for field testing. Apart from this, it must be taken into consideration that in practice an approved vehicle will serve as a basis for further system integration in an FOT.

In this case the approved vehicle is modified for the purpose of field testing. These modifications may – much depending on the character of the modifications – lead to the cancellation of the vehicle's operating licence. Whether this is the case strongly depends on national licensing requirements. These may still be in existence (as is the StVZO = "Straßenverkehrszulassungsordnung" in Germany). According to the provisions therein, the operating license will expire in case of certain modifications (see Sec. 19 para. 2 StVZO).

This does not apply, in case the vehicle parts integrated have a general approval of their own (which is further specified) or have already been approved of as they are – fitted to the vehicle (and have thus been included in the operational licence of the respective vehicle). In order to make the legal effects of modifications manageable, the German Federal Ministry of Transport has established a catalogue of possible modifications and their impact on the vehicle's operating licence (this catalogue is not legally binding). (HENTSCHEL, 2007) The catalogue will provide a good overview in terms of challenges to be overcome for field testing according to the modifications envisaged. Generally speaking, minor changes such as the safe integration of a display, a separate power supply or data logging equipment will not lead to the cancellation of the vehicle's operating licence. The modifications must, however, be made transparent.

6.2 Special regulation for vehicle manufacturers

In this context an important regulation shall be pointed out that will partly exempt vehicle manufacturers (in hold of the type approval certificate for the respective vehicle) from special licensing requirements (see sec. 19 para. 6 StVZO). In Germany, a vehicle that is used for testing by the manufacturer and registered as such, will not be deprived its operating licence, if further parts are integrated for the purpose of testing. (HENTSCHEL, 2007) This regulation will, however, not permit the modification of vehicles privately owned and registered.

6.3 Licensing requirements of “premature” systems/ applications in general

For the purpose of this report a “premature system” shall be considered a system that has so far not been approved of within vehicle type approval and is not separately approved as car accessory either. In order to evaluate such a “premature system” in a Field Operational

Test, a special approval might be required to maintain the vehicles operating licence.

For Germany the law within the federal state is decisive as far as the responsibility of the local public authority is concerned (see Sec. 68 StVZO). The responsible public authority will then decide on the necessity of a report by an officially recognised expert certifying consistency with legal provisions. This will usually not be necessary for manufacturers, see above, section A.6.2.

7 Special licences (exceptional licences within road traffic law)

7.1 Introduction

Further exceptional licences should normally not be necessary for a Field Operational Test – apart from those discussed above in case of modifications on the vehicle’s side. This finding will also apply to the drivers’ driving licences: Driving licences correspond to certain vehicle types and their use will therefore cover any driver assistance as well as any driver information system that does not put full driver’s control into question. And whether data-logging equipment is implemented in a vehicle or not will – if at all – influence the operational licence of the vehicle and does not call for any further special licence.

However, further attention must be raised towards those systems that may intervene beyond full driver’s control. In this case, exceptional licences may be necessary after all.

7.2 Full control of the human driver

The technology available in the past, as well as the Vienna Convention on Road Traffic (1968) have likewise lead to the assumption of the driver’s responsibility to ensure full control over his vehicle. Art. 8 para. 5 and Art. 13 para. 1 of the Vienna Convention explicitly stipulate this full control of the driver over his vehicle “under all circumstances” (Art. 13 para. 1 Vienna Convention on Road Traffic).

The Vienna Convention on Road Traffic formulates a minimum set of requirements in purpose of free (and safe) flow of cross-border transport between the signatory states. The document has had strong influence on the development of national Road Traffic codes and the all-underlying idea of full control of a human driver has thus found its way into many legal provisions concerning road traffic in Germany as well as other countries throughout the EU (and worldwide). In fact, the number of legal provisions based on this idea of full driver’s control went without saying and can even be traced back to national road traffic liabilities (which will again influence insurance issues of such systems, see above, section A.5.4).

These findings are common for the EU at large and must be taken into consideration, in case a system shall be evaluated in a Field Operational Test that overrules full control of the driver. In this case, special legal advice as to the consequences the specific system might bring about will be necessary, as will be the application for exceptional licences. These restrictions will, however, not affect systems that do not put the full control of the driver into question. As such must be considered systems that optimise driver initiated functions (e.g. ABS), advisory systems (e.g. speed alert) and fully overrideable ADAS (e.g. adaptive cruise control). Permissible must further be considered those non-overrideable ADAS that have the same effect as traditional technical limits in vehicle performance (e.g. speed limiters) or intervene in situations that cannot be handled by the driver in time and ensure that the intervention keeps in line with the drivers' intentions and will (e.g. ESP and automatic emergency braking). (ALBRECHT, 2005)

Interventions into driving, however, that counteract to the intentions and will of a driver still able to perform the driving task would bring about legal consequences that cannot be predicted at present. (see "Communication from the Government of the Federal Republic of Germany to the European Commission of 27 June 2007" page 6, stipulating conclusions of the eSafety Conference in Berlin on 5th/6th June 2007)

Therefore a need for an exceptional license will arise whenever a non-overrideable system that does not ensure full control of the driver shall be subject to a Field Operational Test.

8 Ethical rules

Ethics can be considered as a sub-discipline of philosophy and moral principles guiding behaviour, i.e. they help to distinguish, if a certain conduct is right or wrong. Ethical rules apply and must be obeyed in all kinds of research activities on living organisms and, of course, in particular with human beings. The currently most important ethical rules relevant for research but also professional work on human beings have recently been reviewed as subject of the NoE HUMANIST TF 2 activity on ethical laws and guidelines that apply to behavioural experimental studies (HANZLIKOVÁ, 2004). However, in the context of the present report and the planning and preparation of FOTsit does not seem to be necessary to review and discuss all principles which apply when e.g. performing medical or genetic research. Here it seems to be sufficient to refer to the key principles for the evaluation of research which are according to (HANZLIKOVÁ, 2004, p.5):

“Respect for the personality and his or her autonomy, dignity and self-determination.
Beneficence: a commitment to maximise potential benefit and minimise possible risks”

Regarding the planning and performance of FOTs as research projects in the 7th Framework Programme the European Commission makes a clear point when stating: “All research activities carried out under the seventh Framework Programme must be carried out in compliance with fundamental ethical principles” (Decision no. 1982/2006/EC; see <http://ec.europa.eu/research/science-society>). For this reason research proposals shall be evaluated by an independent panel of experts if ethical aspects have been properly addressed. For practical purposes of writing a proposal the EC provides a checklist with critical questions which is designed to help proposers to identify possible relevant ethical

issues (see <http://ec.europa.eu/research/science-society>). With regard to FOTs the following two questions on “Privacy” seem to be most relevant:

Does the proposal involve processing of genetic or personal data?

Does the proposal involve tracking the location or observation of people?

In case of “yes” proposers are required to describe at least the procedures for obtaining informed consent from the persons and the procedures for protecting confidentiality. Moreover, the process of anonymisation or encoding of the data shall be described and it has to be indicated, if the data are used for commercial purposes. These aspects will naturally correspond to legal data privacy provisions, see section A.4.

9 Conclusions

From an overall perspective on legal and ethical issues for FOTs, a number of aspects must be taken into account in terms of planning and accomplishing of such testing. This is mainly due to the significant difference between normal driving and FOTs which lies in the evaluation of possibly immature systems (as far as legally permissible), the great extent of data logged and the unique and possibly unprecedented situation test drivers will be confronted with in open traffic.

To sum up, prohibitive difficulties neither from a legal nor from an ethical point of view are in so far to be expected. As long as the advice provided in this report is considered, potential risks – as far as presently foreseeable – can either be settled, avoided or safely handled. It must, however, further be taken into account that advice provided herein is void of knowledge on the concrete system design and thus specific dangers that might be implied in case of particular systems cannot be covered. It can be expected that such concrete difficulties – apart from those indicated as delicate in the report – can be overcome, this, however, will call for further support on legal and ethical issues within the concrete FOT.

Annex A references

[ALBRECHT, 2005]:

Albrecht, F. (2005). Die rechtlichen Rahmenbedingungen bei der Implementierung von Fahrerassistenzsystemen zur Geschwindigkeitsbeeinflussung. Published in Deutsches Autorecht (DAR), 2005, P. 186-198, Munich, Germany.

[BfD-INFO 1, 2002]:

Editor: Der Bundesbeauftragte für den Datenschutz, Postfach 200112, 53131 Bonn (2002). BfD-Info 1 Bundesdatenschutzgesetz – Text und Erläuterungen –. Leck, Germany. <http://www.datenschutz.bund.de>

[HANZLIKOVA, 2004]:

Hanzlikova, I. (2004). Inventory of ethical laws which apply (at national and EC level) during behavioural experimental studies. NoE HUMANIST, Contract N° 504720, Deliverable 2.1.

[HENTSCHEL, 2007]:

Hentschel, P., König, P., Dauer, P. (2007). Kommentar Straßenverkehrsrecht. Munich, Germany.

[HIMMELREICH/HALM, 2006]:

Editor: Himmelreich, K., Halm, W. Authors: Andreae, M., Becker, A., Bergen, A., Bücken, M., Elvers, R., Engelbrecht, A. Euler, D., Halm, M. Hambloch, R., Hunger, J., Jaeger, L., Kääb, O., Karbach, U. Kreuter-Lange, A., Lehnen, P., Lemor, U. Leser, H., Luckey, J., Mahlberg, L., Müller, M., Nickel, V., Oberpriller, R., Roland, F., Richter, A., Rudolphy, B., Schattenkirchner, S., Schmelcher, M., Steinmeister, M., Schwab, H.-J., Veit, G., Wilms, T., Winkler, T. (2006). Handbuch des Fachanwalts Verkehrsrecht. Cologne, Germany.

[REGAN, 2006, VOL 1]:

Regan, M., Triggs, T., Young, K., Tomasevic, N., Mitsopoulos, E., Stephan, K., and Tingvall, C. (2006). On-Road Evaluation of Intelligent Speed Adaptation, Following Distance Warning and Seatbelt Reminder Systems: Final Results of the Australian TAC SafeCar Project. Volume 1: Report. Monash University Accident Research Centre Report 253. MUARC: Melbourne, Australia.

[REGAN, 2006, VOL 2]:

Regan, M., Triggs, T., Young, K., Tomasevic, N., Mitsopoulos, E., Stephan, K., and Tingvall, C. (2006). On-Road Evaluation of Intelligent Speed Adaptation, Following Distance Warning and Seatbelt Reminder Systems: Final Results of the Australian TAC SafeCar Project. Volume 2: Appendices. Monash University Accident Research Centre Report 253. MUARC: Melbourne, Australia.

[ROSSNAGEL, 2003]:

Editor: Roßnagel A.

Authors: Abel, R.-B., Arlt U., Bär W., Bäumler, H., Breinlinger A., Brühann, U., Bülllesbach, A., Burkert, H., Dembowski B., Dix, A., Duhr, E., Eiermann H., Ernestus, W., Eul, H., Federrath, H., Garstka, H., Groß, T., Gundermann, L., Hansen, M., Hartig, J., Heibey, H.-W., Heil, H., Herb, A., Hillenbrand-Beck, R., Hoeren, T., Holznagel, B., Königshofen, T., Krader, G., Kranz, H.J., Linnenkohl, K., Miedbrodt, A., Müller, U., Naujok, H., Opaschowski, H. W., Petersdorff, U.v., Pfitzmann, A., Poppenhäger, H., Probst, T., Rasmussen, H., Riegel, R., Rieß, J., Schild, H.-H.; Schirmer, H.D.; Schneider, W., Scholz, P., Sokol, B., Sonntag, M., Tinnefeld, M.-T., Tolzmann, G., Topp, C., Trute, H.-H., Wedde, P., Weichert, T., Werner, M., Wollweber, H. Zezschwitz, F.v. (2003). Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung. Munich, Germany.