



IFM
PROJECT
INTEROPERABLE FARE MANAGEMENT

Consensus paper on privacy in transport IFM applications

Deliverable 2.2

Version 4.3

December 2009

Grant Agreement number: IST-2007-214787
Project acronym: IFM PROJECT
Project title: INTEROPERABLE FARE MANAGEMENT PROJECT
Funding Scheme: Support Action
Project Coordinator: John Graham Verity
Head of Compliance
ITSO Limited, United Kingdom

Tel: +44 121 634 3700
Fax: +44 121 634 3737
E-mail: compliance@itso.org.uk
Project website address: <http://www.ifm-project.eu>

For further information please contact:

Work package 2 leader

Michel Arnaud
michel.arnaud@u-paris10.fr

Université Paris Ouest Nanterre La Défense
Labo CRIS InfoCom UFR LLPhi bât L 200 avenue
de la République
92001 Nanterre Cedex
France

Main authors

Michel Arnaud
Michel.arnaud@u-paris10.fr

Authors of Code of conduct for processing
OV-chipkaart personal data
by public transport companies

Authors of terms and conditions for user e-
ticket-chipcard of German transport
companies

Gilles de Chantérac
gilles@chanterac.fr
Jean-Louis Graindorge
jl.graindorge@wanadoo.fr

For further information on the IFM Project please contact:

Coordination

ITSO Ltd.

Phone +44 121 634 3700
Fax +44 121 634 3737
E-mail: compliance@itso.org.uk

Secretariat

TÜV Rheinland Consulting GmbH

Phone +49 221 806 4165
Fax +49 221 806 3496
E-mail: oliver.althoff@de.tuv.com

Visit the webpage www.ifm-project.eu

Table of content

1. Scope of the document	4
2. Executive summary	5
3. Best practices guideline in e-ticketing.....	6
3.1 Definitions	6
3.2 Duty to inform (transparency)	8
3.3 Principles for data processing for fulfilment of transport agreement	8
3.4 Anonymity	11
3.5 Security	13
3.6 Responsibility of privacy	14
3.7 Principles of data processing for personalised marketing	16
3.8 Principles of data processing for research	17
3.9 Retention periods	17
3.10 Rights of the Passenger	18
3.11 Complaints procedure.....	18
ANNEX 1	20
ANNEX 2	22
ANNEX 3	27
ANNEX 4:	32
ANNEX 5	33
ANNEX 6	34
ANNEX 7:	48
ANNEX 8:	58
ANNEX 9:	65

1. Scope of the document

With e-ticketing public transport operators can offer personalised services to their customers which constitute an historical change. Public transport fares used to be anonymous, as the word 'mass transit' suggests and has therefore no ethical implication. The objective of WP2 of IFM project is to propose a privacy model to address traveller's personal data protection issues. This proposed model is compliant with the working paper "e-ticketing in public transport" that was adopted by the international working group on data protection in telecommunication (so-called Berlin Group¹) at its 42nd meeting, 4-5 September 2007. Extracts of this recommendation are given in annex 1.

The objective of this deliverable 2.2 is to provide best practice guidelines agreed upon by relevant professional representatives, which might be also represented by UITP. The document mentioned above from the Berlin Group notes that *"the adoption of a privacy code of conduct should be encouraged. As regards, in particular, processing of data concerning users' movements, the information systems of transportation companies should be designed and implemented by prioritizing the use of anonymous data"*. Best practice guidelines could be seen as a series of recommendations in order to respect a set of rules in agreement with European directive 95-46 as well as national regulations with the common goal to help public transport authorities and operators to build interoperability and provide seamless travel throughout Europe in due respect of citizens privacy. The intention is to reach a positive compromise between respect for privacy, better individualised services and reduced costs of fare management process. This best practice guidelines might also provide European and member state authorities with a framework which facilitates adapting their decision making process to the organisational and professional context of e-ticketing in public transport.

¹ The Group, formed of a number of national data protection authorities and private companies has since 1983, adopted numerous recommendations ("Common Positions" / "Working Papers") aimed at improving the protection of privacy in telecommunications and Internet services.

2. Executive summary

The objective of this document is to propose a common basis to build a consensus on concepts and principles for e-ticketing regulation regarding privacy and giving some directions towards practical implementation. After definition of basic terms, are presented principles such as transparency (duty to inform passenger), fulfilment of transport agreement, anonymity (an option to be offered systematically), security (against misuse of passenger personal data), responsibility for privacy, limits for marketing and research, retention period of personal data, rights of passenger to know, complaint procedures.

The consensus may be difficult to find, as each existing schemes already has its architecture and no one can afford fundamental changes. However a common understanding of these different issues could be the basis for a common set of best practices. It requires participation from representatives of the wider range of countries in Europe. It is hoped that out of the most appropriate set of best practices for traveller's personal data protection, a code of conduct will emerge to be proposed to all European transport operators and agencies.

3. Best practices guideline in e-ticketing

3.1 Definitions

1. **Personal Data:** any information relating to an identified or identifiable natural person.
Additional definition: Is considered as a personal identifier (PID) any set of data describing enough individual characteristic of a person to allow his direct identification, i.e. to find him (official identity, addresses, bank references) or to prove he is himself (biometrics of any sort).
2. **Processing of Personal Data:** any operation or set of operations relating to Personal Data that shall always include the collection, recording, organisation, storage, adaptation or alteration, retrieval, viewing, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of Personal Data.
3. **Data Controller:** Natural person, legal person, administrative body or any other entity, who alone or jointly with others, determines the purpose and means for processing Personal Data.
4. **Data Processor:** Natural person, legal person, administrative body or any other entity who processes personal data on behalf of the controller without coming under the direct authority of that party.
5. **Public Transport Company/Public Transport Companies:** a company that provides public transport services.
6. **Stakeholder:** Any entity that fills one of the roles defined in ISO24014 standard. (i.e. application owner/retailer; product owner/retailer; service operator; security manager, registrar).
7. **Agreement:** (transport) agreement
8. **Passenger:** the (potential) cardholder to which Personal Data relates.
9. **E-ticket Smartcard:** application carrier of the contactless Smart Card type to be used on public transport as a means of payment, access and as a ticket. A balance and one or more travel products and other applications can be stored on this Card.
Additional information: Is considered as an object any hardware or software component in hand of the customer that can be individually managed by integrated fare management systems.
10. **Anonymous Smartcard:** non person-specific smartcard in relation to which no (personal) data about the Cardholder is stored until such time as the Cardholder makes himself known.
11. **Personal Smartcard:** Smartcard to be used by one specific Cardholder whose personal characteristics are displayed on the card, whose personal information is recorded on the chip and whose Personal Data is recorded in the Card Issuer's

systems and the systems of the Public Transport Company where the Cardholder purchased the Smartcard.

12. **Transaction Data:** administrative data that is generated, such as check-in/check-out data and also data relating to the purchase of a (person-specific) travel product, through the purchase and use of the Smartcard by a Passenger and that is recorded in an electronic filing system by the Public Transport Company. Transactions are events in the life cycle of the process that imply an action by the customer. They can relate to the fare system itself or to the related bank orders.
13. **Journey Data:** Selection from Transaction Data (check-in/check-out) that consists of a combination of specific date, time and route information. This Journey Data is necessary for ticket inspection and payment to the carrier for journeys made and to be able to deal with any queries about specific journeys, complaints or requests for compensation/refund for travel products that have/have not been used.
14. **Derived Journey Data:** data derived from Journey Data which concern the following information:
 - Journey frequency;
 - Time since the last journey taken;
 - Peak/non-peak travel;
 - Preferred stations;
 - Preferred routes.

Additional remarks: The date on which and time at which a Passenger travelled and what route he/she took *cannot* be inferred from Derived Journey Data. Journey Data and Derived Journey Data with which the Passenger cannot be identified are not personal data and therefore fall outside the scope of the law, regulations and self-regulation regarding personal data protection.
15. **Card Issuer:** the organisation that is primarily responsible for issuing the Smartcard and for the financial administration of Cardholders' balances.

Additional remarks: The Card Issuer holds the personal data of Passengers with a person-specific Smartcard because the Card Issuer holds the primary responsibility for the issue of the Smartcard, the delivery of specific card services such as blocking cards, for the financial administration of the balance on Passengers' cards and for monitoring the integrity of the Smartcard system.
16. **Marketing:** initiating and maintaining a direct and structured relationship between the Public Transport Company and (potential) customers.
17. **Research:** any form of quantitative and/or qualitative research using statistical or other scientific methods that is intended to be used to make assumptions about target groups or populations at a non individually identifiable level.
18. **Anonymising Procedure:** technical or organisational measures implemented, in the case of repeated Research, to make, following their collection, Personal Data non-identifiable while the data remains linked to the same person throughout the Research.
19. **Privacy manager:** The privacy manager could be an individual within an organisation (head of legal department or data protection compliance officer) who is keeping an overview of all data protection issues within the company. The privacy manager works closely with the data controller.

3.2 Duty to inform (transparency)

One of the key principles of data protection is that Passengers whose personal data are processed are informed about how their personal data will be processed. The Passenger must be informed of who, as the Controller, processes the personal data and the purposes for which it is processed.

Additional information must also be provided as an assurance towards the individual that the data will be handled properly and carefully. To put this into effect, Passengers will be informed of any use of personal data for marketing purposes. Users who do not wish their data to be used in this way will be offered an easy route by which to block the processing of their personal data for this purpose. In this way, the Passenger will always be informed on an application form where personal data is requested of the purposes for which the personal data will be processed. Passengers can also indicate on the form if they do not want their personal data to be used to receive communications. Moreover, the Passenger can at any time exercise the option to block use of their personal data in this way, and an easy method by which Passengers can do this will be offered. The procedure to be followed will be described explicitly in the public transport company's privacy statement. To further put this stipulation into effect, this information will be included not only on the application forms, but will also be made available to Passengers via the websites of the various carriers. Leaflets will also be developed that, in addition to explaining how the Smartcard works, will provide information on data protection.

The Passenger will be informed that the public transport company where the Passenger submitted this application has a record of his/her personal data and the purposes for which it will be processed. It goes without saying that the Passenger will be accorded all legal rights, such as inspection, correction and blocking.

1. If Personal Data is processed, the Public Transport Companies will inform their Passengers of the identity of the Public Transport Company and the purposes for which Personal Data is processed.
2. If Personal Data is also processed for marketing purposes, the Passenger will be informed of this. In addition, at the very least an easy route will be offered by which Passengers can exercise their right to block the use of Personal Data for marketing purposes.
3. The Public Transport Companies will state the above information on the application form for a Personal Smartcard and person-specific products and on their company website.

3.3 Principles for data processing for fulfilment of transport agreement

In the future where paper ticket will disappear, Passengers will need a Smartcard or other medium such as mobile SIM card, USB key, etc... to be able to use public transport. Currently, tickets are often used to provide proof of the right to travel. With the introduction of the Smartcard, the public transport company's electronic recording system will be taken as the definitive source of transactional and other data, unless the Passenger can provide proof to the contrary.

The term agreement above is used in a broad sense. Fulfilment of the agreement could also include ticket inspection during the journey to ensure the ticket is valid. The agreement is often formed by the terms and conditions of carriage in combination with (additional) product terms and conditions.

When a Passenger steps onto a form of public transport, the Passenger enters into a transport agreement with the public transport company with which he/she is travelling. If the Passenger has a person-specific season ticket, then the Passenger has concluded an agreement at an earlier time. When an agreement is concluded this assumes rights and duties for the parties involved: for example, a right for the Passenger to be transported and a right for the public transport company to determine that the Passenger is travelling on the public transport with the right ticket.

It goes without saying that the recording of personal data will be limited only to what is necessary.

Subscriber: The subscriber is the person who subscribed to be registered as a customer in the IFM. As such, the subscriber is the legal person who will be responsible for the use of the resources provided by the IFM such as the media and the applications. Subscribers are also responsible for paying the products when the product includes a billing facility such as post-payment, automatic renewal of products, automatic reloading of stored value.

But many use cases need a subscriber to be registered to at least one of the stakeholders of the Integrated Fare Management system for functional reasons:

- Contractual responsibility
- Billing processes

Subscribers statutes

Statutes data are standardised at the European level by EN 1545-1 defines 20 standard statutes:

adult (1), child (2), student (3), oldAgePensioner (4), disabledNotfurtherpecified (5), disabledVisuallyImpaired (6), disabledHearingImpaired (7), unemployed (8), staff (9), military (10), resident (11), industrialOwnedHaulage (12), busTransportCompany (13), farDistanceTransport (14), localTransport (15), commuter (16), animal (17), object (18), scholar (19).

Codes 20 to 255 are reserved for future national or local use. No particular statute is required to purchase unipersonal products that can be acquired by any customer to get a nominative access right to travel.

Anonymous non-personalized smartcard

In case of anonymous Smartcard, no personal data is known to the public transport company that sells the Smartcard, nor is any personal data known to public transport companies on which Passengers may travel anonymously using a product. However, a situation may arise where a Passenger with an anonymous Smartcard seeks the assistance of the public transport company's customer service department. For example, if the Passenger does not agree with the cost charged for a route travelled. In this case, the Passenger may submit an application for a refund of the amount overcharged to be paid into their bank/giro account, since refunds are never issued in cash. In this situation, in order to deal with the application, the Passenger would have to reveal his/her identity to the public transport company where the application for a refund was submitted. The absence of paper tickets means the public transport company would have to check in the electronic records to see whether this Smartcard had been used to travel on and whether payment was correct. It will not be possible for the public transport company to carry out this type of check at the ticket desk.

Personal smartcard without person-specific agreement

For Passengers who purchase a Smartcard without entering into a person-specific agreement with a Public Transport Company, that Public Transport Company will only

process the Passenger's Personal Data in order to give the Passenger possession of a Personal Smartcard and, if applicable, for the collection of money owed in relation to the purchase of this Personal Smartcard. The only exception to this is when a Passenger wants a personal Smartcard, but does not purchase a person-specific product at the same time. In this specific instance, the public transport company will only process the personal data in order to give the Passenger possession of a personal Smartcard and to collect money owed by the Passenger if the Passenger has to pay for the personal Smartcard. Shortly after that, the public transport company will destroy the personal data. In addition, the organisation that issues the cards will always process the personal data of the holder of a personal Smartcard.

Personal smartcard with person-specific agreement

If a Passenger concludes a person-specific agreement with a Public Transport Company after having applied for a Personal Smartcard, the Public Transport Company with which the Passenger enters into a person-specific agreement will process the Passenger's Personal Data.

When a Passenger purchases a person-specific card on which there is a person-specific product, the public transport company is the Controller. In addition, the public transport company processes, in the role of Data Processor and on the instructions of the Card Issuer, personal data that is necessary to create a person-specific Smartcard and for the Passenger to be able to use this card in the Smartcard system.

In case of a person-specific Smartcard, Passenger's Personal Data are known to the public transport company where the person-specific Smartcard was purchased, the Card Issuer and by every public transport company from which a person-specific travel product is purchased by the Passenger. The public transport company needs this personal data to fulfil the transport agreement (e.g. to check tickets and for payment), but also to be able to deal with queries about specific journeys, complaints or requests for compensation/refund for travel products that have/have not been used.

For person-specific products, it is necessary that the public transport company processes the Passenger's personal data. Often the sale of a person-specific product and a personal Smartcard will go hand-in-hand.

1. It is not permitted to collect and process more Personal Data and Transaction Data than is necessary to fulfil the agreement and to carry out the financial transactions provided for in the agreement.
2. Transaction Data and the Passenger's Personal Data will only be linked when this is necessary.
3. The Public Transport Companies will allow Passengers to view their Transaction Data and/or Journey Data via the internet.
4. If Journey Data needs to be processed for the purposes of providing a service, other than fulfilling the agreement, explicit consent of the Cardholder will be asked.

National Data Protection Commissioners are critical about the possibility of linking Journey Data to Personal Data. Journey Data and Personal Data that identifies the individual should only be linked if this is necessary, for example to resolve a query from a Passenger or a dispute about a (financial) transaction. All such cases refer to specific data only. Specific employees must be appointed within the public transport companies who are responsible for linking such Personal Data where necessary, so as to further limit access to this data.

Passengers will have the option to check the transactions carried out using their Smartcard in a secure environment on the internet. Development of the option to check transactions via the internet will take place in parallel with the roll-out of the Smartcard on public

transport. Passengers can use this information to retrieve overviews for various purposes, including declaring expenses.

When it is necessary to process Journey Data other than for the fulfilment of the transport agreement. In this case, the explicit consent of the Cardholder will be sought to use the Journey Data. This type of service might include giving journey advice. Only if a Cardholder has given their explicit consent will Journey Data be processed to provide this type of service.

3.4 Anonymity

Data on the card are necessary in public transport to perform validation transactions off line and to chain the segments of the trip from check-in to check-out, including eventual transfer points. They can't be "locked" by an authorisation from the customer such as a pin code for practicable reasons and speed of transaction. Furthermore, when applications will be downloaded on smart media with screens, they will be available in clear language to the customer himself.

For technical reasons the number of transactions kept on board of the media will always be limited. In addition, some national data protection authorities have already fixed a maximum number. The fact that the media is personalised or not has no influence upon the risk of private indiscretion, as it is done with the card in hand: *"I know it's my child's card, it was in his school bag"* Private indiscretion from data in the back-office data bases is only possible with complicity from IFM staff that can access or with highly sophisticated hacking.

Consumers must also particularly be protected against undue dissemination of the information about the abnormal events in which they are implied, such as abnormal situation at gates or inspection point, payment incident, etc. so prevent any undue suspicion about their responsibility in that situation. Non-concerned partners mustn't be able to access this information and make use of it against the interest of the customer. These abnormal events may be encoded on the media and in the data bases as a "special event". The corresponding object (medium, secure element, application or product) can also be blacklisted and designated as such in the operational blacklists.

The public transport companies will respect anonymity. This is enshrined in the provision prohibiting any underhand attempts to retrieve personal data on anonymous Cardholders. This is as distinct from the fact that, in order to exercise specific rights, anonymous Cardholders will have to reveal their identity, in which case there is no question of 'underhand methods'. Moreover, a Passenger of this type may still exercise all their legal rights, e.g. to block personal data.

The processing of personal data takes primarily place for internal business processes and secondly to enable to the Smartcard system to function effectively. The exception to this rule is the duty under legislation and regulations to supply personal data. The sensibility of the public to privacy is very dependant from national cultural traditions and history, and legislations differ about the possibility for official bodies and police to access data and make use of it to in the context of inquiries. Passengers do not need to be anxious that other, commercial parties will receive data for their own purposes.

In order to incorporate new understandings and agreements with government and the supervisory authorities, a governing body will be brought into being consisting of public

transport companies. Each company will delegate one representative to sit on this governing body.

1. Public Transport Companies shall respect anonymity. Public Transport Companies shall not make any attempt to retrieve confidential Personal Data from holders of an Anonymous Smartcard.
2. Personal Data from the Smartcard system shall never be supplied to third parties that process this Personal Data for their own purposes, unless the Passenger has either given their explicit consent for this, it is necessary to supply the Personal Data to the Card Issuer, or in case a legal stipulation or court order requires that the Personal Data is supplied.

Options to preserve anonymity

The passengers must have a free decision between anonymous travel and special performances (e.g. best pricing) after the information about the contractually corresponding data processing are presented to them.

- Data for planning purposes and for offer optimisation will be collected anonymously or anonymized.
- If data are needed for special checks or for complaint management, they will be collected and stored under pseudonyms, so that a link without the passenger knowing about it and accepting it is impossible.
- If personal data are written on mobile storage media (smart card) in order to give proof for an eventual complaint, it must be possible for the passenger to delete these data under his own responsibility.

Passengers can select between anonymous and personal travel authorizations (entitlements):

- There are specified anonymous and personal electronic tickets.
- For IN-/OUT-Systems in VDV Germany are specified :
 - Entitlements with stored travel units on the user medium: : eTicket-STRcard
 - Entitlements with anonymous account at the customer contract partner ::eTicket-Card
 - Entitlements connected by payment made by direct debit on Bank account: eTicket-Card
- Collection of data with Check-in/Check-out will be generally done anonymously for accounting, planning purposes and for the travel offer optimisation only necessary data for this purpose will be collected.
- Data for special actions will be stored and assigned to a person (ex: owner of a bank account) only during accounting (billing).
- Personal entitlements will be realised by data set entries into a customer profile held on the user medium as separate object; data will be picked up only within (ticket)controls by inspection staff and will be not stored electronically for further processing
- Personal Data only will be stored on the medium, if the entitlement is non assignable (for example for pupils or students).
- Data will be used on behalf of the complaint management only in connection with the user medium after input of a PIN or in connection with a password input;
- PIN and password will be issued in connection of the issuance of the user medium
- User-referred data on the user media will be overwritten with the next use (max. 20 transactions will be stored on the medium). The German railways data protection commissioner limits it to 10 transactions in the "Touch and Travel Pilot".

3.5 Security

Consumers must be protected against possibilities for hackers to access their data, whatever the objective of the hackers (pride or crime) and whatever the consequences (indiscretion, modification or cloning, with the possibility of usurpation of identity) on the data themselves.

Public transport companies must implement measures to make the processing of data secure. Technical and organisational measures are required to protect the processing of personal data from loss or unlawful processing. The unlawful processing of personal data covers both the organisation (internal) and third parties (external) employed as the Data Processor. Security measures must be implemented both internally and externally and aimed at preventing unauthorised persons from gaining access to the data and that ensuring data is not lost. More stringent security measures must be implemented depending on the nature of the data and whether it is identifiable.

1. The Public Transport Company will store Journey Data separately from Passengers' other Personal Data in both a technical and organisational sense.
2. The Public Transport Company will implement organisational and technical measures to ensure processing takes place securely, taking account of the state of the art technology, the costs and the nature of the Personal Data to be protected.
3. The Public Transport Company will ensure that the Data Processor implements security measures and will inspect these, or arrange for their inspection.
4. The Public Transport Company will require each person who processes Personal Data to sign a confidentiality agreement if and in so far as there is no existing contractual confidentiality.

Example of protection against misuse:

- Application and single entitlements can be blocked by the customer.
- Collected data are usually stored and transferred in coded form for transmission and processing in the IFM systems
 - organizations as numbers which are assigned are confidential
 - locations/stops/stations as number codes, which are not published
- Transaction transmissions take place generally only after cryptographic authentication and secured with a signature (MAC).

Specific processing for data protection

The system components which contain passengers' data are to be fairly protected:

- No possibility for unauthorized users to get access to input data, in particular authentication data by transfer at payment terminals,
- Passengers must be able to pick up contents of the smart card at any time.

Data protection fair organization of the system components:

- Automatic controls and collections of data by terminals will take place only with anonymous authorization data.
- All transactions will be done only after a cryptographic authentication.
- The collection of customer data at vending machines /by Internet will take place only after PIN or password input.
- Service by telephone will take place also only after password authentication.
- Error messages will not contain the error cause in accordance with the specification of the customer interfaces.

Protection against misuse

Precautions (for example blocking the card) must be activated which protect the passenger from loss through the storage medium of data through third party.

3.6 Responsibility of privacy

All participants at Paris workshop on May 20, 2009 agreed on the necessity of complying to the current legal definitions of the controller and processor as defined in Directive 95-46. However the Berlin group and WG29 working party should have their attention drawn upon the fact that in complex applications:

- More than one controller can exist
- The functions of defining the objectives and the one of defining the means may not be in the same hand.
- The statute of sub-processors can't be summarised by considering that sub-contractors are only third parties.

The proposal to define a role of "privacy manager" in IFMs must clearly be understood as a different domain:

The privacy manager would be the function in charge of managing the specific set of rules and regulations that fund the contractual relationship between stakeholders. It is by no means a transfer of the legal responsibility they have as controllers or processors, and it has no authority to interfere in the internal affairs of the stakeholders or to audit their systems or organisations as it had been suggested.

By nature, interoperable e-ticketing systems associate a number of different actors. Each one of them will collect, process and exchange personal data. The French Data Protection Authority, in the single authorization of June 3, 2008 gives a report on this reality: "the interoperability of the systems makes it possible, moreover, to travel with the same ticket on several networks and favours the harmonization of the management of the transport documents"... "within the framework of the interoperable systems, the data of the customer could be exchanged between the urban and interurban networks". In that context, interoperability is only acceptable by customers if they can consider all stakeholders as reliable to respect established and published common privacy rules. The responsibility for privacy relies by nature on the stakeholders as defined in the ISO 24014 role model and the objective of the privacy model is to imply them in a voluntary concern about the subject.

A trusted party is a natural person, a moral person, an institution or a system that can be trusted.

One can trust a technical device which one will be able to hold for reliable, a person held for benevolent or an institution held for reliable. A Party can be trusted without being a "third" party but the complexity of operations inside an IFM leads to a growing number subcontractors external to the partnership.

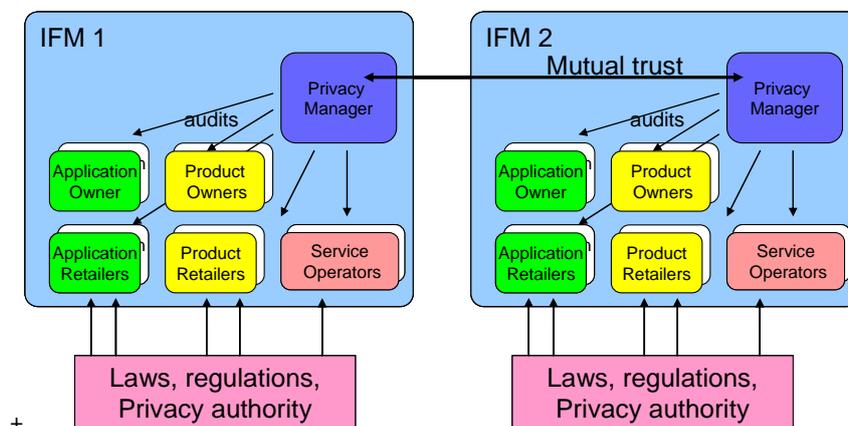
The stakeholders of an IFM, i.e. the legal entities that fulfil the different roles of owners, retailers or service operators, must be trusted parties for privacy. They must therefore set an organisation allowing themselves to refer to each other as privacy respectful parties, because they comply to the charter which is the code of conduct and accept to be audited about it.

Customer contract partners will be obligated in the participation IFM contract to store customer master file data or invoice data in separated systems, so that movement profiles cannot be produced. Data are only united for accounting. Staff of the customer contract partner, who handle personal data, are obliged to keep passenger personal data secret.

Privacy manager

An IFM network should therefore define the entity that will fulfil the role of a “privacy manager”, just as they did chose a “security manager”. The privacy manager can receive a delegation of responsibility for common privacy concerns such as the relations with common suppliers, common sub-contractors or loading agents. He will be in charge to represent the stakeholders of his IFM when discussing privacy issues with an other IFM in setting an agreement for interoperability.

Such an organisation doesn’t conflict with the legal responsibility of each entity, but just stands as a help to it, similarly as quality certifications doesn’t conflict with legal obligations.



Third parties used as sub-contractors in fare management systems

In the technological context, the concept of trusted third party implies an externalisation of responsibility which can be practically implemented by the service being carried out either outside or by a technological device installed in-house as a “black box” and managed by the third party.

Trusted third party may be introduced to prevent the embitterment of responsibilities by being in charge of applying some established and published privacy protection rules acting as firewalls protecting them from transport data being linked with their private identity.

The third party can therefore be either in charge of managing the data themselves or only in charge of locking their access or transfer with appropriate “black boxes”. The concept of trusted third party appeared in the field of cryptography and electronic signature without the term being used by the official texts where the term of “service provider of certification is preferred”. But before any technological context, the ministerial public officers (notaries, bailiffs) or other regulated professions like experts appointed by courts could already be regarded as trusted third parties. The use of trusted third party now applies to a broad range of dematerialized activities (contracts, markets, payment, filing, vote...). In France, a National Federation of Trusted Third parties has been created. It

gathers a number of professionals in the field of technology as well as in the fields of law and economy. The French Data Protection Authority (CNIL) made official the concept of trusted third party on 30 May 2006 by authorizing the experimentation of the Personal medical records (DMP dossier médical personnel) in pilot sites. (See description of process in annex)

The fact for a party to externalise privacy related functions doesn't change its legal responsibility towards the customer, but transfers the technical problem to a supplier and may make the customers feel more confident in the pure intentions of the party.

Third parties using multi-application media aside fare management systems

Tomorrow's technological more important technological change is the possibility to implement various services (tourism, access control ...) and various systems of payment on multi-application supports. Among those, cell phones equipped with NFC technology have already started developing. When where actors whose fields of specialization and interests are different are concerned, secure management in which trust third parties are involved is a central element of the new ecosystem.

Loading agents must be privacy respectful. A particular attention must be attached to the fact that the presence of these external partners must not change the respect for privacy. Unless they apply similar rules, a complete independence of the applications must be guaranteed.

3.7 Principles of data processing for personalised marketing

Mobility is an issue of increasing importance in Europe. Passenger flows are continuously under scrutiny and there is increasing pressure to 'control' Passenger flows. Public transport is faced with the task of attracting more customers onto public transport and/or encouraging customers to travel by public transport more frequently, while improving the efficiency of the services on offer. The public transport companies are introducing various measures to bring the mobility problem under control and retain resources, such as special discount schemes for travel within a specific time period or discounts for those who have reached a particular age. It is not enough just to have promotions that fulfil customers' requirements and generate more business. These promotions also need to be brought to Passengers' attention. The fact that public transport companies 'know' their Passengers means that the relevant information can be sent to this Passenger. Traditional means of communicating this information, such as radio, television and advertising campaigns often do not reach the target group, or do not do so in a cost-effective manner.

The public transport companies can do this on the basis of Derived Journey Data, if the Passenger has not registered an objection to use of his/her Derived Journey Data for marketing purposes. Marketers with the public transport companies will carry out their activities on the basis of these Derived Journey Data. Only after selecting the target group will the Personal Data necessary to approach the Cardholder, i.e. name, address and other data required for communication be processed. Of course, the Cardholder has the right to block their personal data (by opting out).

If a public transport company does not opt for personalised marketing based on Derived Journey Data, then Journey Data is used for this purpose. However, this is only possible if

the explicit consent of the Passenger has been obtained. The Passenger has the right to withdraw his/her consent for the use of Journey Data for personalised marketing at any time.

3.8 Principles of data processing for research

The Smartcard system will enable public transport companies to better match demand and supply (the demand from Passengers for transport services and the service offered by the transport companies). It is not necessary to process Personal Data to do this. This provision specifically governs research that is carried out in relation to Passenger flows and occupancy rates. The aim of this type of research is to better match demand and supply. There is never any requirement with this type of research to have personal data available, and the results of this research cannot be used to approach individuals. The most important of these is that reports of Research may never contain identifying personal data, unless the Passenger has given their explicit consent for this. In the case of long-term Passenger Research, an anonymising procedure will be used to prevent identification in reports. The latter may occur if a specific Passenger flow is the subject of research over a long period. The Anonymising Procedure ensures that the data in the Research always refers to the same Passenger in the Passenger flow, but the identity of the individual Passenger is not known.

1. It is not permitted to collect more Personal Data to carry out the Research than is necessary for the Research.
2. Personal Data shall not be stored or processed in an identifiable form for Research for longer than is necessary.
3. The Research report shall under no circumstances contain information that could identify an individual Passenger unless the explicit consent of the Passenger for this has been obtained.
4. In the case of (long-term) Research using the same Passengers, the Anonymising Procedure must be used to prevent the identification of individual Passengers in the report, unless the same people have given their explicit consent to their participation in long-term Research.

3.9 Retention periods

The public transport companies are conscious that the storage of Smartcard data needs to be covered by more detailed assurances. An essential part of this is the retention period that is applied. However, the public transport companies do not have a free rein in this. In the Netherlands, the normal accounting obligations imposed by the tax authorities apply to public transport companies: in other words, the obligation to retain written records and other data carriers that relate to the business for a period of seven years. To fulfil this requirement, personal data will be stored for this entire period for this specific purpose. In addition, it is necessary to apply a longer retention period for any liability claims that could arise. In this case, the personal data will not be used for any other purposes.

The data will be stored in a dynamic database and a static database. Data that needs to be accessed rapidly will be stored in the dynamic database, such as data required to deal with requests from customers and to allow Passengers to view data and create annual overviews for their own records. Data for this purpose will be available to view via a personal page for eighteen months. Once there is no longer any necessity for the data to be accessed quickly, it will be transferred to a static database. This static database will act as an archive which can only be accessed under specific circumstances.

1. The Transaction Data and Journey Data shall not be retained for longer than is necessary to fulfil contractual and/or legal obligations.
2. Passengers may view their Transaction and Journey Data for a maximum period of eighteen months after the relevant Transaction/Journey took place.

In Germany and in France, the duration of storage of personal data for certain business processes must be as short as possible. In the terminals, stored data should be deleted after successful data transfer in the back office of the customer contracting party or of the service operator.

- It has to be guaranteed by the System operators.
- Time limits will be defined dependent on the business processes and be co-ordinated with the responsible of the data protection commissioner.

3.10 Rights of the Passenger

The rights of the parties involved are based on the rights in relation to data protection conferred by legislation and regulations. This primarily means the Passenger has the right to view his/her personal data at reasonable intervals. Passengers who ask to do so must however identify themselves.

The public transport companies will describe the appropriate procedure in their privacy statement to create clarity for Passengers who want to exercise these rights. Passengers who do not have access to the internet can request information from the public transport company's customer service department. In the case of marketing, the right to block the use of personal data for sales purposes has already been described. As a consequence of blocking, explicit consent to use Journey Data and personal data for sales purposes can no longer be asked.

1. The Passenger shall be entitled to view at reasonable intervals what Personal Data is recorded by the Public Transport Company.
2. The Passenger shall be entitled to improve, add to, remove or protect the Personal Data that has been recorded if this data is factually incorrect, or incomplete or irrelevant for the purpose or purposes of processing or is otherwise processed contrary to legal requirements.
3. A Public Transport Company shall only respond to the above requests if the person making the request has properly identified himself.
4. Passengers shall have the right at all times to block the use of their Personal Data held by a Public Transport Company for marketing purposes. The Public Transport Company shall inform Passengers of their right to object whenever a message for personalised Marketing purposes is sent.
5. The Public Transport Company shall define clear procedures for handling the types of requests detailed above.
6. The Public Transport Companies shall always comply when a Passenger objects to the use of their Personal Data for marketing purposes.
7. All Public Transport Companies shall include details on their websites of how the Passenger can exercise the above rights.

3.11 Complaints procedure

Passengers who believe that their rights are not respected as a result of an action or omission on the part of the public transport company can submit a complaint to that public transport company. The public transport company will investigate the complaint within four weeks and inform the Passenger of the outcome of this investigation. If the Passenger

is not informed within the stated term or the Passenger considers that the complaint has not been dealt with satisfactorily, a complaint may then be submitted to the DPA. The option to complain to a Disputes Committee is offered in the Netherlands distinct from the legal avenues open to the Passenger to complain to the DPA or to bring a case before the courts.

1. If a Public Transport Company acts contrary to the provisions of the DPA regulations for public transport, the Passenger may, in the first instance, submit a complaint to the Public Transport Company about the action or failure that has given rise to the complaint. The Public Transport Company will investigate the complaint and inform the Passenger of their findings within four weeks.
2. If the Passenger is not informed of the findings within the period specified in the previous part, or considers that the complaint has not been dealt with satisfactorily, the Passenger may then submit a complaint to the DPA.

ANNEX 1

Extracts from Working Paper about E-Ticketing in Public Transport adopted by the G29 working party *at the 42nd meeting, 4-5 September 2007, Berlin*

Innovative e-ticketing systems work by means of electronic cards, usually personalised, that are predominantly used for transport services but may increasingly be used to purchase related services (e.g. to pay commuter parking fees).

Smart cards contain a chip to store information, including personal information (which may include a chip identifier, the number of the user's subscription contract as well as time, date and code number of the card validation device); in some cases they operate via RFID/Near Field Communication (NFC) technology.

The use of such cards therefore entails the processing of several items of directly and/or indirectly identifiable personal information:

- at the time the cards are issued to users;
- each time the cards are used, thanks to the identifiers that are associated with every subscriber and collected by the validation devices to be subsequently stored (possibly in real time) in the databases of transport companies.

Special attention should be paid in this context to the information related to the so-called validation data, whose processing - in particular the storage of the time and place of validation - allows tracking the individual users' movements and whereabouts.

Privacy Impact Assessment

The information systems of transport companies should be designed and implemented by taking into account the customers' right to protection of their personal data; generally speaking, they should reconcile the right to free movement of individuals with the requirements of effective public transportation.

Anonymity

The Public Transport Authority (PTA) or Transport Company should provide alternative ways for customers to travel anonymously (without undue obstacles), e.g. cash or an anonymous e-ticket.

Where anonymity cannot be offered for technical reasons, the following recommendations have to be observed:

Privacy Policy and Transparency

PTAs or transport companies using e-ticketing systems should provide data subjects with unambiguous information on the processing of personal data which they carry out. Data subjects should be in a position to easily understand all the specific purposes sought by the companies, what items of personal information concerning them are collected and stored, and how such information is used.

Data Minimization and Retention Period

As regards, in particular, processing of the data concerning users' movements, the information systems of transport companies should be designed and implemented by prioritizing the use of anonymous data. If (directly or indirectly) identifiable information is used, this information should be stored for the shortest possible period (and erased automatically thereafter), and account should be

taken of the lawful purposes to be achieved via the processing - as a rule, the information in question should not be retained for longer than a few days after being stored.

Security

Security for accessing personal data should include an audit system to prohibit the misuse of information.

Transport companies should ensure that the privacy of registered users is guaranteed when making their databases accessible to partners or even their own employees.

Marketing

APTA or transport company should obtain the free and informed prior consent of customers for the use of personal data for its own marketing purposes or associated partner's usage of information for unsolicited marketing towards the traveller. This consent should be distinct from the acceptance of the general contractual obligations.

Proof of Payment

As far as proof of payment for individual journeys is required e.g. for refunds or tax allowances, privacy-friendly solutions should be offered.

Code of Conduct

The adoption of a privacy code of conduct should be encouraged. As regards, in particular, processing of the data concerning users' movements, the information systems of transportation companies should be designed and implemented by prioritizing the use of anonymous data.

System Design

System design should be such as to separate the personal information from travel information (two component model). Central storage should be reserved for aggregate data and/or anonymous transactions.

The Cardholder should be able to control information concerning his use of the card.

ANNEX 2

Answers provided at the Paris workshop on May 20, 2009

Participants in the Paris workshop on May 20, 2009 were asked to discuss the following questions in order to build a consensus if possible.

Answering question 1:

Would it be possible and opportune in IFM systems, to create a “privacy manager” to play a role in relationship with the ones of controller, processor, third party ?

Participants observed that the directive 95-46 does not define any role for a “privacy manager”.

It was agreed on the fact that first of all definitions provided by the directive 95-46 should be applied.

Indeed, the “controller” is precisely defined in precise terms by the European directive 95/46/CE, as being *“the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”* (Article 2 Directive 95/46).

The processor too: he *“is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”* (Directive article 2) ; the controller is thus, legally the only , juridically responsible person and in the case of traveller’s complaint he *“may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage”* .

Concerning liability, article 23 of the directive provides that:

- 1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.*
- 2. . The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.*

The controller” could act alone or jointly with others (Directive, article 2) processing personal data on each behalf and always under his responsibility. If a traveller complains, the controller will be the only liable person.

Under these conditions, the question is to know if it is possible to derogate conventionally from these provisions to transfer the responsibility to an entity which would not be the “controller” according to the definition provided by the EU Directive

There exists also another legal obstacle with the designation of a “privacy manager” in a e-ticketing system grouping several transport operators. Indeed, the national law of each operator is applicable since *“the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable (Article 4 Directive).*

In respect of the definition of personal data, it was discussed that data relating to the traveller is not personal data as long it is not possible to find out through them the traveller's identity. The question was whether it takes a disproportionate effort to relate travelling data to a specific individual natural person. The fact that a third party may hold identifying data is not decisive: this third party may be prohibited by law to reveal the identifying data. Consequently, the mere fact that a third party is holding identifying data is not sufficient.

Answering question 2: What restrictions brings travelling anonymously regarding status verification, special fares and fraud control?

This question raised in the French CNIL which stated on different occasions that the respect of privacy the freedom of going and coming anonymously implied that the travellers have a true choice between displacements anonymous or personal, which supposes that those are carried out under equivalent conditions.

Consequently, an anonymous card alternative to the personalised one has been introduced in several e-ticketing systems in France. However the anonymous card cannot be used for personalised products like season tickets.

The same situation in the Netherlands: in the Dutch OV-chip card system, travellers can make a choice between an anonymous card and a personalized card. The anonymous card is a fully fledged OV-chip card, holding an electronic purse. Consequently, the traveller can just as well travel anonymously in the OV-chip card system in the Netherlands. Only if the traveller wishes to load personalized products on its cards, such as personalized season tickets or, for example, an auto reload agreement (to automatically reload the e-purse), then the traveller needs to have a personalized OV-chip card.

This situation (accepting the alternative of an anonymous card but restricted to normal fares) is explained by the following reasons:

- differences in rates (age, number of travels)- inspection purpose (fraud control): the delays of travel data storage vary from one country to another: 48h in France and 16 months in England
- purse on card (reloading procedures)
- after sales services,
- tax rebates to be arranged with authorities
- use of a card with a certain rate in another country with the same special rate/

Answering question 3:

What post-payment implies in terms of keeping traveller's personal data?

There was a debate on the opportunity of introducing post-payment. Some participants noted that there is no need or urgency to pay before hand. Therefore, post-payment is going to be more and more used. Dutch representatives did not think that 'post-payment is going to be more and more used'. They saw a development towards preloading of money on an e-purse and the widespread use of pre-loaded cards in public transport

Data which are necessary to make post-payment possible are related to traveller's identity and his means of payment. Besides a traveller does not want to share his data but to have

a one-to-one relationship; for instance, it could be with the transport company, the credit card company or the mobile phone company.

In case of international travel, there may be several reasons why stakeholders need to have access to personal data, e.g., in any case the cardholder uses a personalized product or service from a stakeholder.

There are risks at two levels: between operators and between traveller and his home operator. Therefore an IFM organisation should issue guidelines in order to define rules that should apply to protection of traveller's personal data.

Answering question 4:

What type of personal data to be made available on media?

Participants first marked the difference between data ON the card and IN the card. For example, in Germany, the full name of the traveller is written ON the card but is not fully registered IN the card; only three first letters of the name followed by XXX appear on the card, which allows fraud control.

Participants also raised the issue of data protection offered by card manufacturers. They took example of NFC cell phone where information on chip is read at a distance by a reader and sent to telephone operator back office systems. Information on chip is useful to identify customers and offer them special rebates for example. However, specific commitments should be asked from telephone operators in order to build confidence with travellers using their NFC phones as transport media.

During the discussion after the reporting:

- SNCF reminded that the issue of sharing personal data should not only include transport but also new services (multi services application - for example health, cycle rental, etc..), therefore the privacy manager should control all services and not only transport services.

- In multi-application systems, security system is splitting secure zones that cannot be linked. However, phone companies may identify existing applications on the media because they allocate memory space and can make links. Several levels of security are needed, depending on application type (transport, bank, ..) but users should have the choice to share or not their personal data, for instance to take advantage of a special offer.

- Data are not necessarily shared between operators but operators still have to be in contact with each other to solve conflicts. Sometimes conflicts of interest could arise between two operators: if a customer does not pay his phone bill, could he still use this mobile for transport?

- SNCF added that, in France, there are two lists: a list of unpaid bills and a list of bad payers (black listed). Only card numbers can be shared and their access is limited.

In Germany, similarly blacklists contain only card numbers and are shared with restrictions.

In the Netherlands, there are several blacklists: product blacklist, e-purse blacklist and card blacklist (on customer demand, in case of lost or stolen card).

Presentation of national legislation and applications

The afternoon discussion during the Paris workshop on May 20, 2009 was organised around a presentation of each country's legislation represented among participants: Belgium, the Netherlands, Germany, UK, France, in order to get specific answers from the point of view of how PTOs handle personal data protection national legislations.

Belgium

Belgian e-ticketing system (especially in Brussels) is asking authorization from Belgian DPA to keep travellers personal data for 12 months. There is an anonymous card being offered as an option for travellers but for one travel trip only. Information kept on the card: customer id, contract number, validated fare, 3 last travels. Blacklisting is allowed to control fraud. The overall objective is to extend e-ticketing to all Belgian provinces (Walloon as well as Flemish).

The Netherlands

The Netherlands have developed OV chip card in is rolled out all over the Netherlands in any type of public transport. Translink is offering a card which can be anonymous or contain personal data (customer contract number, etc...) Translink has agreed on a privacy Charter with PTOs. The Privacy Charter is part of the contractual framework that all PTO's participating in the system adhere to. An agreement with the Dutch Data Protection Authority regarding the use by PTO's of traveller's data for direct marketing purposes has been concluded. A selected set of aggregated data may under very strict conditions, and only in specific cases be used for Direct Marketing purposes without prior consent, unless the traveller makes use of its right to opt-out. There is still a debate with the fiscal authorities about the Legal requirement to keep data for 7 years.

Germany

VDV Germany has developed a e-ticketing system which relies on PTOs and/or PTAs data controllers working under the supervision of each Lander DPA as well as federal DPA for private and public companies as well. If they are common customer contracts among PTOs and PTAs, conservation of personal data is justified in case of civil and penal trials. They are no personal data for children up to 14 years old because they cannot be sentenced by a penal court and they are not able to make a proper contract. Personal data storage in automatic processing is legal as long as the purpose exists. They are no central storage for travellers personal data as well as transaction data. Application retailer (primary customer contract partner) is the only one to store personal data. Transaction data and personal data have to be stored separately. There is no direct marketing purpose without customer agreements who can decide which data are to be shared among PTOs and PTAs. There are no privacy complaints for the moment. Blacklisting is done by the application owner. There is no media identifiers therefore card numbers can be used as pseudonyms since there is no link to back offices

France

French personal data protection law of 2004 has modified the notion of nominative data and introduce the notion of personal data which has included all data with any link (direct or indirect) that allows identifying a person.

Personal data can be gathered and kept only during a specific delay (48h for transport data) before a a process of anonymisation makes it impossible to identify a traveller.

These anonymised data can be kept in a specific data base. For example RATP keeps 2 data bases which are separated: one with personal data, one with transaction data with links between the 2 to be severed by hash coding and anonymisation preventing to find again the link. For RFID chips, the same approach is enforced.

In the discussion, from the Dutch PTOs point of view this French approach is contrary to the development of personalized services. In France however, anonymised transaction data can be used for statistical analysis and for ever after. A key transforms the nominative data (name) into a code (always the same number for the same name,) which enables statistics. In case of post-payment, CNIL found a solution: out of 3 types of information related to travel transaction data such as place, day and hour, only 2 types of information can be kept together with traveller name. It helps to keep a right balance between traveller's personal data protection and commercial purposes.

United Kingdom

In UK and especially for ITSO, each of 200 PTOs or more having bought concessions has its privacy managers. ITSO services imply that info to be kept on the national card includes: photograph, expiry date, card number. What is encoded: card number and identifier. 10 millions cards are used presently.

Guidance on personal data handling on media has been issued by the information commissioner with a minimum amount of regulations. If blacklisting is done in back offices, self regulations prevail. There is no risk assessment being made, no audit performed by DPA and no intention to do so. Third party is not a notion which is classified.

Provisional conclusion

From the general discussion, it appears that the outcome should not be a privacy charter but a code of best practices. If privacy managers or officers can meet twice a year to exchange ideas and solutions, privacy compliance officers should be under the responsibility of data controllers and third parties should enter written agreements with data controllers as well. Security measures and confidentiality protection are under the exclusive responsibility of data controllers according to European law as well as national laws. In France, there is only one data controller per process, but they could be several in a PTOS network such as IFM scheme according to European law.

Anonymous accessibility can be solved with an anonymous fare card even taking into account specific status (unemployed for example): 3 technical solutions are thought over by CNIL (French DPA) and will be released soon. In order to gather as much info as possible on national regulations and how PTOs apply them, a call is made to all participants for further contributions. A note is to be written by Dutch partners on Dutch DPA law and how it is implemented by PTOs.

ANNEX 3

Privacy regulations for electronic ticketing in transport services in France

Jean-Louis Graindorge, URBA 2000 September 2008

For a better understanding of the issue of privacy in the field of electronic ticketing, it is necessary to describe the solutions that the French data protection Authority (CNIL) provided by its interpretation of the act of 6 January 1978 on Data Processing, Data Files and Individual Liberties amended by the Act of 6 August 2004.

This description is facilitated by the publication, in July 2008, of a so-called "autorisation unique (single authorization) which, when it is respected, exempts the authors of a system from a prior approval.

An analysis of the essential provisions of this document is presented.

1° Principles of the French act on Data Processing, Data Files and Individual Liberties

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

Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means,

Personal data filing system shall mean any structured set of personal data which are accessible according to specific criteria.

The data must be collected for determined, explicit and legitimate purposes and do not have to be excessive taking into consideration these purposes. They must be preserved in a form allowing the identification of the people that are concerned during a period of time which shall not exceed the duration necessary to the finalities for which they are collected and treated. Beyond this duration the data must be the subject of a process of anonymisation accepted by the French Data Protection Authority.

2° Application of the principles as regards e-ticketing

2.1. The recommendation n° 03-038 of September 16, 2003

The French Data Protection Authority was brought to take a first recommendation in 2003 which concerned NAVIGO which is the e-ticketing system of the Ile de France region managed by the French railways (SNCF) and the public transport operator (RATP).

In this recommendation, The French Data Protection Authority notes that the use of nominative smartcards involves the collection, at the time of the validation, of the

journeys of the card holder: the date, hour, and place of validation or correspondence and the number of the card are memorized; and the number of the card is indirectly personal because it makes possible the identification of its holder whose coordinates appear in the customers' database.

Consequently, journeys made when using the card are not anonymous any more, they can be traced and this traceability of displacements is likely to conflict two fundamental freedoms: the right to freedom of movement and the right to respect of private life. In accordance with the principles pointed out above, the recommendation of CNIL relates to the identification of the finalities of the data processing, the anonymisation of the data, the duration of data conservation in case of fraud fixed at two days or, if the fraud is proven, during time of instruction by the court.

It also affirms that it is highly desirable that the possibility of circulating in an anonymous way is maintained by means of an e-ticketing system. In other words, the subscribed customers of the public transport service must be able to choose between a nominative and an anonymous smartcard. Moreover, in an opinion of April 8, 2004, the Authority considered that the choice of an anonymous card should not generate overcost compared to the choice of nominative card. This last recommendation was at the origin of the creation in Ile de France, in September 2007, of the "Pass Navigo Découverte"

On the basis of the principles expressed by this recommendation, CNIL had on several occasions to formulate an opinion on other e-ticketing systems implemented on the national territory.

2.2. The single authorization AU 015

2.2.1. Definition

a) The concept of single authorization is envisaged by article 26-3 of the act of 6 January 1978 on Data Processing, Data Files and Individual Liberties amended by the Act of 6 August 2004.

It describes the rules applicable to the files and data processing which aim at the same finality and the categories of data and recipients.

When such an authorization exists, it is not necessary any more for any one setting up a system to carry out the formalities of declaration or prior approval as far as this system is conform to the regulations of the authorisation. In that case, a declaration of conformity is enough. In the contrary case, if one derogates from it completely or partially, prior approval is again necessary.

b) On June 3, 2008 the CNIL made a decision of single authorization (n° AU-015) concerning the implementation of automated treatments of personal data for the management of e-ticketing applications by transport authorities and operators. This authorization was published in the French Official journal of July 2, 2008.

2.2.2. Content

The preparation of this authorization was relatively long. Its provisional last version gave place to comments of the public transport stakeholders.

Bases

In addition to the question of the traceability of displacements, the French Data Protection Authority based the legitimacy of its intervention on the article 25-1-4 of the national act on Data Processing, Data Files and Individual Liberties which subjects to prior approval “the automated treatments, which because of their nature, or their finalities, are likely to exclude people from the benefit of a right, a service or a contract”

This analysis differs from the operators' viewpoint who consider that article 25-1-4 is not applicable because the cancellation of the contract between the customer and the operator in the case of unpaid is part of the bilateral contract concluded between the client and the operator which generates reciprocal and interdependent obligations between the contractors (the payment being counterpart of the right to travel). There is thus no unilateral exclusion. In addition, people are always able to use normal tickets

Purposes of the use and the data processing of personal data

The purposes described in the authorization are more clearly described than in 2003 and are close the wishes of the authorities transport operators.

- Management, delivery and use of the transport documents
- Management of commercial relations
- Fraud management
- Statistical analyses
- Measurements of service quality

Processed personal data

a) Operators underlined the difficulty in referring to an exhaustive list of data, taking into account commercial and technological evolutions. They recommended to gather these data in five generic functional categories without necessarily drawing up a precise list of the contents of these categories:

- Person data
- Commercial data
- Distribution data
- Validation and control data
- Safety. Data

b) The national Authority did not follow this suggestion and operated a classification in three precisely broken up categories:

A first category concerns management, delivery, use of electronic transport documents, statistical analyses, measurement of quality, fraud management and the detection of the technological fraud. One finds there:

- Person data (civil statute, data in relation with the payment, socio-professional data, identity card in the event of remote payment, photo, proof of residence)
- Sale data (client number, history, type of subscription)
- After sale data (dates of beginning and end of validity of the card, card number)
- Validation data (date, hour, location)
- Control data (the reason for the inscription on a file of exclusion according to a closed list).

The second category concerns the management of the social tariffs (free transport documents or cheap rate): schooling; handicap; benefit of a social allowance; age; incomes; large family... The operators pointed out that it would be useful to take into account data making it possible to justify certain current or future tariff reductions resulting from sustainable mobility policies. The CNIL uses the term “of social allowance” which will have certainly to be extensively interpreted to include these reductions.

The third category relates to the management of the unpaid services: in addition to information of civil statute and banking, the amount of unpaid, the number of the cheque or bank card, the date of the rejection, the reason in the shape of a closed list indicating for example the absence or the insufficiency of provision, or the invalid means of payment; the number of warnings before suspension of the subscription, data related to the payment. This enumeration seems to take into account the wishes expressed by the operators.

Restrictions of use and conservation of the data

- The number of events of validation recorded in the card must be limited to four and can be extended to six for needs of interoperability. On this point the French Authority’s position evolved compared to its position of 2003 when it noted: “the number of events of validation recorded in the card, which currently varies between two and six, would have, at the time of the passage to the next generation of cards, to be limited to four”.
- The validation data can only be associated with the data of identification of the subscriber (for example its card number) within the framework of the treatment of the detection of the fraud. In this case, the Authority confirms its recommendation of 2003 and envisages a possibility of conservation during 48 hours.
- These data, non associated with the card numbers or some other means of direct identification of the subscribers, can be collected for statistical purposes. Information making it possible to identify the user can be associated with the date and hour of validation, provided the relative information with the place are removed within the one month limit.

Example of the KORRIGO card operated in the Rennes metropolitan area

Three different databases:

- *The first contains the card numbers and the hours of validation;*
- *The second contains the place and the day of validation;*
- *The third is the database customers.*

It is not possible to bring closer the first and the second databases because there is no more common denominator (the number of the card).

The second database (place and day of the validation) is used for the statistics; the first database (n° of chart and hour) is used for the after sales, in particular in the event of loss or theft).

Duration of data conservation

- a) All the client's data can be preserved during the time of the contractual relation, and beyond this date during two years for statistical and commercial purposes. The request from the operators for a six years delay has not been taken into account.
- b) Validation data are submitted to anonymisation in the near future. This anonymisation is carried out either by the complete suppression of the card number, or by the joint suppression of the date, the hour and the location or by the application to the card number of a cryptographic hash algorithm (today all e-ticketing applications use cryptography for data anonymisation).

Information of the customers

- a) the single authorization envisages: "The people likely to be registered in the treatment of unpaid must be informed about it:
 - at the time of the signature of subscription contract
 - before being recorded in the database of unpaid and stopping the validity of the transport document.

If a delay is given at the time of an injunction to pay, the person in charge of treatment must mention on the letters of revival the time available to the person concerned to regularize his situation, as well as the consequences of stopping the validity of one's card.

- b) Insofar as such an obligation would be heavy and complex to implement, operators had wished that information preliminary to the record in the unpaid database not be maintained. The Authority did not take this request into consideration.

Conclusion

The single authorization of June 2008 temporarily concludes a very long debate between transport actors and privacy experts. It makes possible to reconcile the technological advance and the respect of the right of the individuals.

ANNEX 4:

Role of a trusted third party to manage Personal medical records (DMP dossier médical personnel) (France, 2006)

The Trusted third party acts as a fire-wall protecting individuals from medical facts being unduly linked to their private identity.

Article 5 of the law of August 13, 2004 provides that a decree, taken after opinion of the CNIL, determines the conditions under which an identifier can be used for the opening of the personal medical records.

The CNIL emitted in 2006 the following opinion:

“A specific health identifying number, called NIS, will identify the patient and will guarantee against the doubles and the collision risks. Its creative process by the GIP-DMP (Group of Public interest Personal medical records) will utilize a trusted third party, the “Caisse des dépôts et consignations”, member of the Board of directors of the GIP-DMP. This number will be, as the CNIL wished it, disconnected from the social security number.
”

The NIS makes it possible each one to have access to the medical data. The NIS must be able to make it possible to identify the patient without ambiguity. The following process was set up for the needs of the experimentation:

To make open a DMP, a patient signs a contract with a company agreed to record and to process health data.

A doctor gives to the voluntary patient a form to opening of contract DMP made up of two sheets.

On the first sheet, there is a number of form. The patient registers his name, his first name, his social security number and his address.

The second form is the contract with the company which indicates the name and address of the patient but not his social security number.

The identity is checked by connection to the national directory of identification of the recipients of the health insurance (répertoire national d'identification des bénéficiaires de l'assurance maladie), a number of form is then associated; the trusted third party recovers the number of form and calculates the NIS by means which guarantee its unicity. By preserving the list of the numbers of already calculated NIS, the trusted third party is able to verify that the NIS does not already exist. Once the NIS is calculated, the number of form and the NIS are sent to the company which places the NIS in front of the number of the contract form. Only the trusted third party manages the creation of the NIS. By the process which has just been written, the social insurance number and the NIS never cohabit.

ANNEX 5

Multi-application in IFM

Multi-application is based upon an imbricate hierarchy of physical and/or virtual objects (products, encoded in applications, loaded in secure elements, embedded or inserted in physical media), each of them being capable to host not only a certain number elements of inferior rank (e.g. one application can host different products).

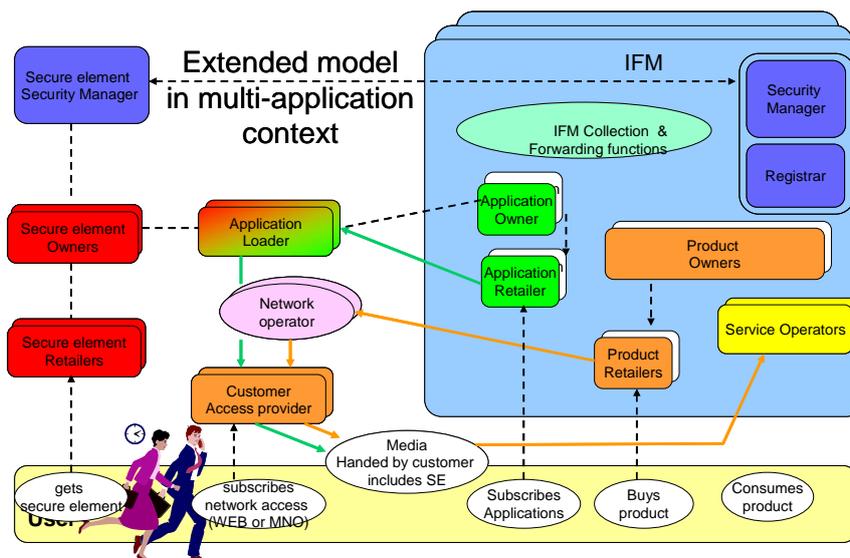
The media itself can have different forms, such as multi-application cards, NFC USB keys, NFC mobile-phones are the most likely first solutions.

Global Platform and Java specifications provide the secured infrastructure and software to guarantee the independence of the applications inside the secure elements. This allows independent applications and businesses.

But, inside the IFMs and more over between them, new issues arise about the organisation. The role model from ISO 24014-1 must be extended to account with the secure element and media as new objects, having in their turn one owner and being retailed by different retailers.

An extended model is currently discussed in CEN-ISO groups for multi-application contexts. In this extended role model, external entities cooperate with the stakeholders of the IFM and participate in moving data and eventually in owning and retailing the secure element and media that may not be issued by the IFM itself as native transport cards were.

The image below, extracted from the discussions of the most recent CEN TC278- WG8- SG5 meeting pre-figures what the extended role model could be. Possibilities to load applications and products directly from the contactless interface is not shown.



ANNEX 6

Code of conduct for processing OV-chipkaart personal data by public transport companies (The Netherlands)

OV-chipkaart [public transport smart card]

This document has been provided after a workshop at Translink Amersfort on October 2, 2009

Adopted on 21 June 2007 by Mobis and deposited with the Court in The Hague on 10 July 2007 under number 50/2007.

Amended on 6 February 2009 and adopted by the public transport companies that accept the OV-chipkaart and, at their request, deposited by KNV with the Court in The Hague on 13 February 2009 under number 16/2009.

Translated by NS Dutch Railways in cooperation with law firm Kennedy Van der Laan

Do not use this text as a model

This Code of Conduct has been drafted specifically for official redress procedures in the Netherlands. Consequently, the text is rather formalistic and does not describe real company behaviour. For example, the Code states that it is not permitted to collect more data than is necessary, referring to the use limitation principle in EU data protection directive 95/46/EC. Obviously, such a ban is not a best practice but simply mandatory by rule of law. The Code *does* contain references to true best practices, however. Dutch redress possibilities on themselves are working examples. Most important is probably the fact that the Code provides an outline for organizational and technical measures for [embedded privacy protection](#) (Privacy by Design) within e-ticketing networks.

KNV - Koninklijk Nederlands Vervoer is the employers' organisation for professional freight transport and professional passenger transport: public transport, taxi and coach transport.

Mobis - industry association of companies involved in collective passenger transport by road and rail - dissolved on 31 December 2008.

Contents

1. Preamble
 2. Definitions
 3. Description of the sector and scope of application
 4. Duty to inform
 5. Principles for data processing if a personal OV-chipkaart is purchased without a person-specific product being purchased at the same time
 6. Principles of data processing for fulfilment of agreement
 7. Principles of data processing for personalised marketing
 8. Principles of data processing for research
 9. Retention periods
 10. Security
 11. Rights of the Passenger
 12. Complaints procedure
 13. Other matters
- Explanation

1. Preamble

The Public Transport Companies that sign this Code of Conduct, having regard to the fact that:

1. It should be transparent for Passengers who use a (personal) OV-chipkaart which organisations process personal data as Controllers;
2. The Public Transport Companies believe that transparency for Passengers will result in greater confidence in the OV-chipkaart system on the part of Passengers;
3. Greater confidence will act as an incentive to use the (personal) OV-chipkaart;
4. It is desirable to draw up more detailed agreements within the context of legislation and regulations relating to the protection of personal data, with regards to the processing of personal data generated by the use of the personal OV-chipkaart
5. This Code of Conduct applies exclusively to the relationship between Cardholders/Passengers and Public Transport Companies;
6. The Public Transport Companies may amend the Code of Conduct in the light of social developments and applications of the OV-chipkaart;
7. The Code of Conduct provides for an independent Disputes Committee;
8. The Code of Conduct was evaluated in 2008 and revised on the basis of new understandings and agreements;

have adopted the following Code of Conduct:

2. Definitions

1. Personal Data: any information relating to an identified or identifiable natural person.
2. Processing of Personal Data: any operation or set of operations relating to Personal Data that shall always include the collection, recording, organisation, storage, adaptation or alteration, retrieval, viewing, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of Personal Data.
3. OV-chipkaart: application carrier of the contactless smart card type to be used on public transport as a means of payment, access and as a ticket. A balance and one or more travel products and other applications can be stored on this Card.

4. Anonymous OV-chipkaart: non person-specific OV-chipkaart in relation to which no (personal) data about the Cardholder is stored until such time as the Cardholder makes himself known.
 5. Personal OV-chipkaart: OV-chipkaart to be used by one specific Cardholder whose personal characteristics are displayed on the card, whose personal information is recorded on the chip and whose Personal Data is recorded in the Card Issuer's systems and the systems of the Public Transport Company where the Cardholder purchased the OV-chipkaart.
 6. Public Transport Company/Public Transport Companies: a company that provides public transport services in the Netherlands in the sense of the *Wet personenvervoer 2000* [Dutch Passenger transport act].
 7. Controller: the natural or legal person, or public body that alone or jointly with others determines the purposes and means of the processing of Personal Data.
 8. Data Processor: a person who processes Personal Data on behalf of the Controller without being subject to the Controller's immediate authority.
 9. Passenger: the (potential) Cardholder to which Personal Data relates.
 10. Research: any form of quantitative and/or qualitative research using statistical or other scientific methods that is intended to be used to make pronouncements about target groups or populations at a non individually identifiable level.
 11. Anonymising Procedure: the technical or organisational measures implemented, in the case of repeated Research, to make, following their collection, Personal Data non-identifiable while the data remains linked to the same person throughout the Research.
 12. *Wet Bescherming Persoonsgegevens*: Dutch data protection act, Law Gazette 2000, no. 302.
 13. Disputes Committee: De *Geschillencommissie Openbaar Vervoer* [public transport disputes committee], Postbus 90600, 2509 LP The Hague, the Netherlands.
 14. Transaction Data: the administrative data that is generated through the purchase and use of the OV-chipkaart by a Passenger and that is recorded in an electronic filing system by the Public Transport Company.
 15. Journey Data: Transaction Data that consists of a combination of specific date, time and route information.
 16. Derived Journey Data: new data derived from Journey Data from which new data cannot be inferred where someone was at a specific time.
 17. Cardholder: natural person who uses an OV-chipkaart.
 18. Marketing: the creation and maintenance of a direct, structured relationship between the Public Transport Company and (potential) customers.
 19. Card Issuer: the organisation that is primarily responsible for issuing the OV-chipkaart and for the financial administration of Cardholders' balances.
 20. Agreement: (transport) agreement
-
3. Description of the sector and scope of application
 1. This Code of Conduct applies to Public Transport Companies that have signed this Code of Conduct and that accept the OV-chipkaart.
 2. This Code of Conduct applies to the processing of Personal Data by Public Transport Companies that takes place as a result of the purchase and use of an OV-chipkaart by a Passenger using Public Transport.

 4. Duty to inform

1. If Personal Data is processed, the Public Transport Companies will inform their Passengers of the identity of the Public Transport Company and the purposes for which Personal Data is processed.
 2. If Personal Data is also processed for marketing purposes, the Passenger will be informed of this. In addition, at the very least an easy route will be offered by which Passengers can exercise their right to block the use of Personal Data for marketing purposes.
 3. The Public Transport Companies will state the above information on the application form for a Personal OV-chipkaart and person-specific products and on their company website.
-
5. Principles for data processing if a Personal OV-chipkaart is purchased without a person-specific product being purchased at the same time
 1. For Passengers who purchase an OV-chipkaart without entering into a person-specific agreement with a Public Transport Company, that Public Transport Company will only process the Passenger's Personal Data in order to give the Passenger possession of a Personal OV-chipkaart and, if applicable, for the collection of money owed in relation to the purchase of this Personal OV-chipkaart.
 2. If a Passenger concludes a person-specific agreement with a Public Transport Company after having applied for a Personal OV-chipkaart, the Public Transport Company with which the Passenger enters into a person-specific agreement will process the Passenger's Personal Data.
-
6. Principles of data processing for fulfilment of agreement
 1. It is not permitted to collect and process more Personal Data and Transaction Data than is necessary to fulfil the agreement and to carry out the financial transactions provided for in the agreement.
 2. Transaction Data and the Passenger's Personal Data will only be linked when this is necessary.
 3. The Public Transport Companies will allow Passengers to view their Transaction Data and/or Journey Data via the internet.
 4. If Journey Data needs to be processed for the purposes of providing a service, other than fulfilling the agreement, explicit consent of the Cardholder will be asked.
-
7. Principles of data processing for personalised marketing
 1. Subject to the provisions of section 11, part 4 and section 11, part 6, the Public Transport Companies may use two methods for personalised marketing, as described in part 2 and part 3 of this section.
 2. Public Transport Companies may process data for personalised marketing under the following conditions:
 - a. Marketing only takes place on the basis of Derived Journey Data
 - b. Public Transport Companies collate Derived Journey Data on the basis of Journey Data. Derived Journey Data does not contain any Journey Data.
 - c. For personalised marketing, Public Transport Companies do not have access to Journey Data other than for the purposes of collating Derived Journey Data.
 3. Public Transport Companies may process Journey Data for personalised marketing if the Passenger has given their explicit consent for this in accordance with section 6, part 4.

8. Principles of data processing for Research

1. It is not permitted to collect more Personal Data to carry out the Research than is necessary for the Research.
2. Personal Data shall not be stored or processed in an identifiable form for Research for longer than is necessary.
3. The Research report shall under no circumstances contain information that could identify an individual Passenger unless the explicit consent of the Passenger for this has been obtained.
4. In the case of (long-term) Research using the same Passengers, the Anonymising Procedure must be used to prevent the identification of individual Passengers in the report, unless the same people have given their explicit consent to their participation in long-term Research.

9. Retention periods

1. The Transaction Data and Journey Data shall not be retained for longer than is necessary to fulfil contractual and/or legal obligations.
2. Passengers may view their Transaction and Journey Data for a maximum period of eighteen months after the relevant Transaction/Journey took place in order to fulfil section 6, part 3 of this Code of Conduct.

10. Security

1. The Public Transport Company will store Journey Data separately from Passengers' other Personal Data in both a technical and organisational sense.
2. The Public Transport Company will implement organisational and technical measures to ensure processing takes place securely, taking account of the latest technology, the costs and the nature of the Personal Data to be protected.
3. The Public Transport Company will ensure that the Data Processor implements security measures and will inspect these, or arrange for their inspection.
4. The Public Transport Company will require each person who processes Personal Data to sign a confidentiality agreement if and in so far as there is no existing contractual confidentiality.

11. Rights of the Passenger

1. The Passenger shall be entitled to view at reasonable intervals what Personal Data is recorded by the Public Transport Company.
2. The Passenger shall be entitled to improve, add to, remove or protect the Personal Data that has been recorded if this data is factually incorrect, or incomplete or irrelevant for the purpose or purposes of processing or is otherwise processed contrary to legal requirements.
3. A Public Transport Company shall only respond to the above requests if the person making the request has properly identified himself.
4. Passengers shall have the right at all times to block the use of their Personal Data held by a Public Transport Company for marketing purposes. The Public Transport Company shall inform Passengers of their right to object whenever a message for personalised Marketing purposes is sent.
5. The Public Transport Company shall define clear procedures for handling the types of requests detailed above.

6. The Public Transport Companies shall always comply when a Passenger objects to the use of their Personal Data for marketing purposes.
7. All Public Transport Companies shall include details on their websites of how the Passenger can exercise the above rights.

12. Complaints procedure

1. If a Public Transport Company acts contrary to the provisions of this Code of Conduct, the Passenger may, in the first instance, submit a complaint to the Public Transport Company about the action or failure that has given rise to the complaint. The Public Transport Company will investigate the complaint and inform the Passenger of their findings within four weeks.
2. If the Passenger is not informed of the findings within the period specified in the previous part, or considers that the complaint has not been dealt with satisfactorily, the Passenger may then submit a complaint to the *Geschillencommissie Openbaar Vervoer* in accordance with the Disputes Committee's regulations. If there is no response from the Public Transport Company within the specified period, the complaint must be submitted within four weeks of the term specified in the previous part elapsing and, in the case of a complaint about the response received, the complaint must be submitted within four weeks of receipt of that response, unless the complainant makes a reasonable case that this cannot reasonably be expected of him/her.
3. If the Disputes Committee handles the complaint on the basis of the Code of Conduct for processing by Public Transport Companies of OV-chipkaart Personal Data, the Privacy Compliance Officer, if the Public Transport Company has one, or similar representative of the Public Transport Company against whom the complaint is made will be heard in the proceedings.

13. Other aspects

1. Public Transport Companies shall respect anonymity. Public Transport Companies shall not make any attempt to retrieve confidential Personal Data from holders of an Anonymous OV-chipkaart.
2. Personal Data from the OV-chipkaart system shall never be supplied to third parties that process this Personal Data for their own purposes, unless the Passenger has either given their explicit consent for this, it is necessary to supply the Personal Data to the Card Issuer, or in case a legal stipulation or court order requires that the Personal Data is supplied.
3. This Code of Conduct will be evaluated at regular intervals and amended if necessary. This will be carried out by a governing body consisting of the Public Transport Companies.

This Code of Conduct has been deposited with the Court at The Hague on 13 February 2009 under number 16/2009.

Explanation

This Code of Conduct is limited in its current version to Personal Data obtained through the purchase and use of the OV-chipkaart by Passengers on public transport. It is not inconceivable that at a later date, when the drafters of the Code of Conduct have built up more experience of the handling of personal data, that this Code of Conduct could be extended to all processing of personal data within public transport companies or to other applications of the OV-chipkaart beyond public transport. This Code of Conduct has been

Page 39 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

designed so that it can be adapted and grow in line with applications and social developments in the area of the protection of personal data, public transport and use of the OV-chipkaart.

Introduction

The public transport companies in the Netherlands have started the process of introducing the OV-chipkaart. The introduction of the OV-chipkaart heralds a new era in which it will be easier for Passengers to travel on and pay for public transport.

In addition, the OV-chipkaart is being used by public transport companies as an 'access key' to metro and train stations. Controlled access will contribute to public safety on public transport.

There are two versions of the OV-chipkaart, an anonymous and a personal OV-chipkaart. The choice of which type of OV-chipkaart to purchase depends on the Passenger's requirements and the type of season ticket purchased. The option will also be available at all times to use public transport anonymously.

The new OV-chipkaart system makes it necessary to process personal data. The *Wet Bescherming Persoonsgegevens* applies to the processing of personal data. Other laws that affect the processing of personal data, such as the *Wet personenvervoer 2000*, also apply to public transport companies.

The public transport companies have taken the initiative to document the processing of personal data in an unambiguous and transparent way in this Code of Conduct.

This Code of Conduct describes how public transport companies handle personal data in their various business processes. The public transport companies are acting in the belief that in drafting this Code of Conduct they have the backing of the Minister for Transport, Public Works and Water Management who, on 1 November 2006, called for the drafting of a Code of Conduct for the processing of personal data by public transport companies. Defining a Code of Conduct provides an easy way for Passengers to find out the how personal data is processed by the public transport companies. Moreover, this does not release the public transport companies from their legal obligations to inform Passengers if personal data is processed.

Code of Conduct and the *Wet Bescherming Persoonsgegevens*

The *Wet Bescherming Persoonsgegevens* provides for the drafting of a code of conduct. In the Code of Conduct, the abstract standards from the *Wet Bescherming Persoonsgegevens* and other laws, in so far as they apply to the sector, are specified in greater detail. A Code of Conduct may also provide for an independent facility to settle disputes between Controllers and Passengers about the processing of personal data. The public transport companies have decided that, for the time being, this Code of Conduct should not be a Code of Conduct under the *Wet Bescherming Persoonsgegevens*. The public transport companies would initially like to build up some experience with the Code of Conduct and the OV-chipkaart system. The Code of Conduct provides for the independent settlement of disputes via the *Geschillencommissie Openbaar Vervoer*. A simple route is provided by which Passengers can submit complaints to the Disputes Committee - after having submitted a complaint to the public transport company - about the way in which the public transport companies comply with this Code of Conduct. The Disputes Committee has specific knowledge of public transport and therefore has expertise in the settlement of disputes that concern public transport. The Passenger has the final choice of whether to put a dispute before the Disputes Committee. The Passenger also has the option to put a dispute before the supervisory authorities or the courts.

The public transport companies do not rule out the possibility that this Code of Conduct may be put before the *College bescherming persoonsgegevens* [personal data protection supervisory authority] at a later date.

Procedure

Page 40 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The Board of Mobis took a decision to draft this Code of Conduct on 14 December 2006. The Code of Conduct was drafted by the transport terms and conditions working group. The annual general meeting of Mobis adopted this Code of Conduct on 21 June 2007.

Evaluation in 2008

In 2008 the text of the Code of Conduct was evaluated against developments in the privacy code of the *College bescherming persoonsgegevens*. As part of this evaluation new understandings and agreements were embedded in the text. The Code of Conduct was adopted in amended form by the DOC (Directeurenoverleg OV-chipkaart - Directors' consultative committee for public transport smart card) on 6 February 2009. Mobis ceased to exist on 1 January 2009. The public transport companies sign this Code of Conduct individually. KNV acted as the platform for the evaluation.

The OV-chipkaart in the light of the *Wet Bescherming Persoonsgegevens*

The introduction of the OV-chipkaart affects the quantity and nature of the (personal) data that a public transport company collects and how the public transport company handles this data. The *Wet Bescherming Persoonsgegevens* specifies standards for the processing of personal data. In addition, the *College bescherming persoonsgegevens* has a supervisory role under the *Wet Bescherming Persoonsgegevens*.

The public transport companies are faced not only with the requirements of the *Wet Bescherming Persoonsgegevens* when it comes to the processing of personal data. Obligations under other legislation, such as the *Wet personenvervoer 2000*, also make it necessary for public transport companies to process personal data.

Delineation: What type of processing is subject to this Code of Conduct?

Public transport companies process personal data about Passengers, such as season ticket holders. The purposes of said processing are to fulfil the agreement, to inform Passengers of changes in the timetable and to draw Passengers' attention to other/new travel products. In addition, public transport companies have been given the task in the *Nota mobiliteit* [mobility policy document] of promoting the use of public transport. This Code of Conduct applies to (personal) data that is generated by the purchase and use of the OV-chipkaart by Passengers with a public transport company that accepts the OV-chipkaart. Moreover, it goes without saying that the *Wet Bescherming Persoonsgegevens* also applies to this Code of Conduct.

Therefore, systems in which personal data originating from the OV-chipkaart system is processed, plus any other personal data, are subject to this Code of Conduct. This includes systems that are used to fulfil agreements, to supply services, and for marketing and statistics.

Section 2 Definitions

This section relates to the definition of terms that are relevant for the functioning of the Code of Conduct. Terms from the definitions section of the *Wet Bescherming Persoonsgegevens* have been used. Some terms have been changed to suit their application in practice, for instance the term data subject has been replaced by the term Passenger. The Code of Conduct only applies to personal data. Journey Data and Derived Journey Data with which the Passenger cannot be identified are not personal data and therefore fall outside the scope of the law, regulations and self-regulation regarding personal data protection.

The public transport companies will often act as Controller. This is because they determine the purposes for which and means by which personal data is processed.

In the Code of Conduct, a distinction is made between Transaction Data and Journey Data. Transaction Data is all data that is generated through the use of the OV-chipkaart in the OV-chipkaart system. This is administrative data, such as check-in/check-out data, but also data relating to the purchase of a (person-specific) travel product. Journey Data is a specific group of Transaction Data; Journey Data is a selection from the Transaction Data

(check-in/check-out) that is combined with the specific date, time and route data. This Journey Data is necessary for ticket inspection and payment to the carrier for journeys made and to be able to deal with any queries about specific journeys, complaints or requests for compensation/refund for travel products that have/have not been used.

Examples

When a Passenger purchases a person-specific card on which there is a person-specific product, the public transport company is the Controller. In addition, the public transport company processes, in the role of Data Processor and on the instructions of the Card Issuer, personal data that is necessary to create a person-specific OV-chipkaart and for the Passenger to be able to use this card in the OV-chipkaart system.

The OV-chipkaart system provides for two types of OV-chipkaart: an anonymous and a person-specific card. In the case of a person-specific OV-chipkaart, the personal data is known to the public transport company where the person-specific OV-chipkaart was purchased, the Card Issuer and by every public transport company from which a person-specific travel product is purchased by the Passenger. The public transport company needs this personal data to fulfil the transport agreement (e.g. to check tickets and for payment), but also to be able to deal with queries about specific journeys, complaints or requests for compensation/refund for travel products that have/have not been used. In addition, the public transport company where the person-specific OV-chipkaart with a person-specific product was purchased will inform the Cardholder that the OV-chipkaart should be renewed at the time at which the OV-chipkaart expires. As a result of this, Passengers with a person-specific OV-chipkaart from the public transport company but without a person-specific product from that public transport company will not be informed that the OV-chipkaart has expired by the public transport company where the person-specific OV-chipkaart was purchased. The Card Issuer holds the personal data of Passengers with a person-specific OV-chipkaart, because the Card Issuer holds the primary responsibility for the issue of the OV-chipkaart, the delivery of specific card services such as blocking cards, for the financial administration of the balance on Passengers' cards and for monitoring the integrity of the OV-chipkaart system.

In the case of the anonymous OV-chipkaart, no personal data is known to the public transport company that sells the OV-chipkaart, nor is any personal data known to public transport companies on which Passengers may travel anonymously using a product. However, a situation may arise where a Passenger with an anonymous OV-chipkaart seeks the assistance of the public transport company's customer service department. For example, if the Passenger does not agree with the cost charged for a route travelled. In this case, the Passenger may submit an application for a refund of the amount overcharged to be paid into their bank/giro account, since refunds are never issued in cash. In this situation, in order to deal with the application, the Passenger would have to reveal his/her identity to the public transport company where the application for a refund was submitted. The absence of 'paper' tickets means the public transport company would have to check in the electronic records to see whether this OV-chipkaart had been used to travel on and whether payment was correct. It will not be possible for the public transport company to carry out this type of check at the ticket desk.

The Passenger will be informed that the public transport company where the Passenger submitted this application has a record of his/her personal data and the purposes for which it will be processed. It goes without saying that the Passenger will be accorded all legal rights, such as inspection, correction and blocking.

Section 3 Description of the sector and scope of application

This Code of Conduct applies to transactions carried out using the OV-chipkaart with public transport companies that have a Framework Agreement with Trans Link Systems BV in

Page 42 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

respect of participation in the OV-chipkaart system. The Code of Conduct only applies to transactions that that can be deemed personal data. An OV-chipkaart for which no details about the Passenger are known falls entirely outside the scope of this Code of Conduct.

Section 4 Duty to inform

One of the key principles of data protection is that Passengers whose personal data are processed are informed about how their personal data will be processed. The Passenger must be informed of who, as the Controller, processes the personal data and the purposes for which it is processed. Additional information must also be provided that is necessary to provide an assurance towards the individual that the data will be handled properly and carefully. To put this into effect, Passengers will be informed of any use of personal data for marketing purposes. Users who do not wish their data to be used in this way will be offered an easy route by which to block the processing of their personal data for this purpose. In this way, the Passenger will always be informed on an application form where personal data is requested of the purposes for which the personal data will be processed. Passengers can also indicate on the form if they do not want their personal data to be used to receive communications. Moreover, the Passenger can at any time exercise the option to block use of their personal data in this way, and an easy method by which Passengers can do this will be offered. The procedure to be followed will be described explicitly in the public transport company's privacy statement. To further put this stipulation into effect, this information will be included not only on the application forms, but will also be made available to Passengers via the websites of the various carriers. Leaflets will also be developed that, in addition to explaining how the OV-chipkaart works, will provide information on data protection.

Section 5 Principles for data processing if a personal OV-chipkaart is purchased without a person-specific product being purchased at the same time

In the future, Passengers will need a OV-chipkaart to be able to use public transport. There are two types of OV-chipkaart: the personal OV-chipkaart and the anonymous OV-chipkaart. For person-specific products, it is necessary that the public transport company processes the Passenger's personal data. Often the sale of a person-specific product and a personal OV-chipkaart will go hand-in-hand. The only exception to this is when a Passenger wants a personal OV-chipkaart, but does not purchase a person-specific product at the same time. In this specific instance, the public transport company will only process the personal data in order to give the Passenger possession of a personal OV-chipkaart and to collect money owed by the Passenger if the Passenger has to pay for the personal OV-chipkaart. Shortly after that, the public transport company will destroy the personal data. In addition, the organisation that issues the cards, Trans Link Systems BV, will always process the personal data of the holder of a personal OV-chipkaart.

Section 6 Principles of data processing for fulfilment of agreement

When a Passenger steps onto a form of public transport, the Passenger enters into a transport agreement with the public transport company with which he/she is travelling. If the Passenger has a person-specific season ticket, then the Passenger has concluded an agreement at an earlier time. When an agreement is concluded this assumes rights and duties for the parties involved: for example, a right for the Passenger to be transported and a right for the public transport company to determine that the Passenger is travelling on the public transport with the right ticket. The introduction of the OV-chipkaart will do away with paper tickets. Currently, tickets are often used to provide proof of the right to travel. With the introduction of the OV-chipkaart, the public transport company's electronic recording system will be taken as the definitive source of transactional and other data, unless the Passenger can provide proof to the contrary. The term agreement above is used in a broad sense. Fulfilment of the agreement could also include ticket inspection during the journey to ensure the ticket is valid. The agreement is often formed

by the terms and conditions of carriage in combination with (additional) product terms and conditions.

It goes without saying that the recording of personal data will be limited only to what is necessary.

The *College bescherming persoonsgegevens* has been critical about the possibility of linking Journey Data to Personal Data. Journey Data and Personal Data that identifies the individual should only be linked if this is necessary, for example to resolve a query from a Passenger or a dispute about a (financial) transaction. All such cases refer to specific data only. Specific employees must be appointed within the public transport companies who are responsible for linking such Personal Data where necessary, so as to further limit access to this data.

Passengers will have the option to check the transactions carried out using their OV-chipkaart in a secure environment on the internet. Development of the option to check transactions via the internet will take place in parallel with the roll-out of the OV-chipkaart on public transport. Passengers can use this information to retrieve overviews for various purposes, including declaring expenses.

Section 6, part 4 provides for a situation in which it is necessary to process Journey Data other than for the fulfilment of the transport agreement. In this case, the explicit consent of the Cardholder will be sought to use the Journey Data. This type of service might include giving journey advice. Only if a Cardholder has given their explicit consent will Journey Data be processed to provide this type of service.

Section 7 Principles of data processing for personalised marketing

Public transport companies fulfil a role in society. This much is clear from the name alone - public transport. Mobility is an issue of increasing importance for the Netherlands. Passenger flows are continuously under scrutiny and there is increasing pressure from politicians to 'control' Passenger flows. Public transport is faced with the task of attracting more customers onto public transport and/or encouraging customers to travel by public transport more frequently, to stagger use of services at peak times and to improve the efficiency of the services on offer. The public transport companies are introducing various measures to bring the mobility problem under control and retain resources, such as special discount schemes for travel within a specific time period or discounts for those who have reached a particular age. It is not enough just to have promotions that fulfil customers' requirements and generate more business. These promotions also need to be brought to Passengers' attention. The fact that public transport companies 'know' their Passengers means that the relevant information can be sent to this Passenger. Traditional means of communicating this information, such as radio, television and advertising campaigns often do not reach the target group, or do not do so in a cost-effective manner.

The public transport companies can do this in two ways: on the basis of Derived Journey Data, as specified in section 7, part 2 whereby the Passenger can register an objection to use of the Derived Journey Data for marketing purposes and on the basis of section 7, part 3, providing that the Cardholder's explicit consent has been obtained.

Part 2

The public transport companies may work on the basis of Derived Journey Data. What does this mean?

The public transport companies derive new data from the Journey Data for marketing purposes. It is not possible to deduce from this new data where someone was at any given moment. Agreement has been reached with the *College bescherming persoonsgegevens* on the following set of Derived Journey Data that can be used:

Journey frequency;

Time since the last journey taken;

Page 44 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Peak/non-peak travel;
Preferred stations;
Preferred routes.

Therefore, the date on which and time at which a Passenger travelled and what route they took *cannot* be inferred from Derived Journey Data. It has also been agreed with the *College bescherming persoonsgegevens* that any additions to the above set of data will be discussed with the *College bescherming persoonsgegevens*.

Marketers with the public transport companies will carry out their activities on the basis of this Derived Journey Data. Only after selecting the target group will the Personal Data necessary to approach the Cardholder, i.e. name, address and other data required for communication be processed. Of course, the Cardholder has the right to block their personal data (by opting out).

The use of Derived Journey Data for personalised marketing will not take place before 2010.

Part 3

If a public transport company does not opt for personalised marketing based on Derived Journey Data, then Journey Data is used for this purpose. However, this is only possible if the explicit consent of the Passenger has been obtained in accordance with section 6, part 4 of the Code of Conduct. The Passenger has the right to withdraw his/her consent for the use of Journey Data for personalised marketing at any time. The use of Journey Data for personalised marketing will not take place before 2010.

Section 8 Principles of data processing for Research

The OV-chipkaart system will enable public transport companies to better match demand and supply (the demand from Passengers for transport services and the service offered by the transport companies). It is not necessary to process personal data to do this. This provision in the Code of Conduct specifically governs research that is carried out in relation to Passenger flows and occupancy rates. The aim of this type of research is to better match demand and supply. There is never any requirement with this type of research to have personal data available, and the results of this research cannot be used to approach individuals. This provision includes the classic principles of research as set down in the *Gedragcode voor Onderzoek & Statistiek* [code of conduct for research and statistics], approved by the *College bescherming persoonsgegevens* on 18 February 2004 (Law Gazette 2004, no. 36). The most important of these is that reports of Research may never contain identifying personal data, unless the Passenger has given their explicit consent for this. In the case of long-term Passenger Research, an anonymising procedure will be used to prevent identification in reports. The latter may occur if a specific Passenger flow is the subject of research over a long period. The Anonymising Procedure ensures that the data in the Research always refers to the same Passenger in the Passenger flow, but the identity of the individual Passenger is not known.

Section 9 Retention periods

The public transport companies are conscious that the storage of OV-chipkaart data needs to be covered by more detailed assurances. An essential part of this is the retention period that is applied. However, the public transport companies do not have a free rein in this. The normal accounting obligations imposed by the tax authorities apply to public transport companies: in other words, the obligation to retain written records and other data carriers that relate to the business for a period of seven years. To fulfil this requirement, personal data will be stored for this entire period for this specific purpose. In addition, it is necessary to apply a longer retention period for any liability claims that could arise. In this case, the personal data will not be used for any other purposes. The data will be stored in a dynamic database and a static database. Data that needs to be accessed rapidly will be stored in the dynamic database, such as data required to deal with requests from

Page 45 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

customers and to allow Passengers to view data and create annual overviews for their own records. Data for this purpose will be available to view via a personal page for eighteen months. Once there is no longer any necessity for the data to be accessed quickly, it will be transferred to a static database. This static database will act as an archive which can only be accessed under specific circumstances.

Section 10 Security

Public transport companies must implement measures to make the processing of data secure. Technical and organisational measures are required to protect the processing of personal data from loss or unlawful processing. The unlawful processing of personal data covers both the organisation (internal) and third parties (external) employed as the Data Processor. Security measures must be implemented both internally and externally and aimed at preventing unauthorised persons from gaining access to the data and that ensuring data is not lost. More stringent security measures must be implemented depending on the nature of the data and whether it is identifiable.

Section 11 Rights of the Passenger

The rights of the parties involved are based on the rights in relation to data protection conferred by legislation and regulations. This primarily means the Passenger has the right to view his/her personal data at reasonable intervals. Passengers who ask to do so must however identify themselves.

The public transport companies will describe the appropriate procedure in their privacy statement to create clarity for Passengers who want to exercise these rights. Passengers who do not have access to the internet can request information from the public transport company's customer service department.

In the case of marketing, the right to block the use of personal data for sales purposes has already been described. As a consequence of blocking, explicit consent to use Journey Data and personal data for sales purposes can no longer be asked.

Section 12 Complaints procedure

Passengers who believe that this Code of Conduct is not being observed as a result of an action or omission on the part of the public transport company can submit a complaint to that public transport company. The public transport company will investigate the complaint within four weeks and inform the Passenger of the outcome of this investigation. If the Passenger is not informed within the stated term or the Passenger considers that the complaint has not been dealt with satisfactorily, a complaint may then be submitted to the *Geschillencommissie Openbaar Vervoer* in accordance with the Disputes Committee's regulations. Further information is available at www.degeschillencommissie.nl.

The option to complain to the Disputes Committee is distinct from the legal avenues open to the Passenger to complain to the *Geschillencommissie Openbaar Vervoer* or to bring a case before the courts. Consideration by the Disputes Committee is in addition to the existing options. The Disputes Committee will not consider disputes or delay the consideration of a dispute if the Passenger has submitted a complaint to the *College bescherming persoonsgegevens* or has put the matter before the courts.

Section 13 Other aspects

A section is included at the end of the Code of Conduct covering a number of aspects relating to the protection of Passengers' privacy.

The public transport companies will respect anonymity. This is enshrined in the provision prohibiting any underhand attempts to retrieve personal data on anonymous Cardholders. This is as distinct from the fact that, in order to exercise specific rights, anonymous Cardholders will have to reveal their identity, in which case there is no question of 'underhand methods'. Moreover, a Passenger of this type may still exercise all their legal rights, e.g. to block personal data.

The processing of personal data takes primarily place for internal business processes and secondly to enable to the OV-chipkaart system to function effectively. The exception to this rule is the duty under legislation and regulations to supply personal data. Passengers do not need to be anxious that other, commercial parties will receive data for their own purposes.

This Code of Conduct will be evaluated at regular intervals in order to incorporate new understandings and agreements with government and the supervisory authorities in the Code. For this purposes, a governing body will be brought into being consisting of public transport companies as intended in the *Wet personenvervoer 2000* and/or the *Concessiewet* [public transport franchises act]. Each company will delegate one representative to sit on this governing body.

Published at the request of the public transport companies by
Koninklijk Nederlands Vervoer (KNV)
Spui 188
2511 BW The Hague
Postbus 19365
2500 CJ The Hague
Telephone +31 (0)70 375 17 51
Fax +31 (0)70 345 58 53
Internet www.knv.nl

ANNEX 7:

PHR2006 - Federal Republic of Germany 18/12/2007

Constitutional Privacy Framework in Germany

Article 10 of the Basic Law (or Grundgesetz, the German Constitution) states: "(1) Privacy of letters, posts, and telecommunications shall be inviolable. (2) Restrictions may only be ordered pursuant to a statute. [1] Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament."

In a 1983 case against a government census law, the Federal Constitutional Court formally acknowledged an individual's "right of informational self-determination," which is only limited by the "predominant public interest." The central part of the verdict stated, "Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them." [2] This landmark court decision derived the "right of informational self-determination" directly from Articles 1(1) and 2(1) of the Basic Law, which declare personal rights (Persönlichkeitsrecht) to freedom are inviolable. Attempts to amend the Basic Law to include a right to data protection were discussed after reunification, when the Constitution was revised, and were successfully opposed by the then-conservative political majority.

Data Protection Framework

Germany has one of the strictest data protection laws in the European Union. The world's first data protection law was passed in the German Land of Hessen in 1970. In 1977, a Federal Data Protection Act (Bundesdatenschutzgesetz or BDSG) followed, which was reviewed in 1990, amended in 1994 and 1997. The final major revision took place in 2002 to be in line with the EU Data Protection Directive. [3] The general purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his personal data. The Act covers collection, processing and use of personal data by public federal authorities and state administrations (as long as there is no state regulation and insofar as they apply federal laws), and by private bodies, if they rely on data-processing systems or non-automated filing systems for commercial or professional use. The majority of federal statutes that have an impact on personal information and privacy contain references to the Federal Data Protection Act if they do not carry special sections on the handling of personal data themselves.

The 2001 revisions to the BDSG include regulations on personal data transfers abroad, video surveillance, anonymization and pseudonymization, smart cards, and sensitive data collection (relating to race or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, and sexual orientation). It grants data subjects greater rights of objection. It also states that, apart from public bodies, private companies are now also required to appoint a data protection officer if they collect, process, or use personal information. Without this responsible person, each introduction of automated data processing must be registered with the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The BDSG also provides that consent from the individual

whose data is collected is required after full disclosure of data collection and its consequences. The German Parliament renewed its request for secondary legislation on auditing requirements.[\[4\]](#)

A general revision of the BDSG has been considered for 2005, but the Legislative process is still ongoing.[\[5\]](#) Albeit an expert report on the modernization of the data protection law was published in 2001,[\[6\]](#) there has been no visible legislative progress. This reputable report recommends reducing the number of laws governing specific details of privacy protections and creating one general statute, which would only refer to more detailed regulations where necessary.[\[7\]](#) An ideal statute would provide general rules about the use of privacy-friendly techniques, data security, privacy standards, control of data processing, and self-regulation tools.[\[8\]](#) On February 17, 2005, the German Parliament (Bundestag) called upon the government to swiftly submit a draft for a Federal Data Protection Act incorporating these recommendations.[\[9\]](#)

All of the sixteen Länder have their own specific data protection regulations that cover the public sector of the Länder administrations. All Länder have adopted new data protection laws pursuant to the EU Data Protection Directive.[\[10\]](#) Each Land also has a data protection commissioner to enforce the Länder data protection acts.[\[11\]](#) Moreover, it falls within the competence of the Länder DPAs to supervise the compliance of the private sector with the Federal Data Protection Act. The federal and Länder data protection officers hold conferences on a regular basis to exchange information and issue common statements.[\[12\]](#)

Another important federal law in Germany is the G-10 Law, which imposes limitations on the secrecy of certain communications as provided in Article 10 of the Basic Law (Grundgesetz).[\[13\]](#) Under the G-10 Law, parliamentary control commissions, established on federal and Länder's level, supervise the surveillance powers of intelligence agencies. As amended in 1994 by the Crime Fighting Law (Verbrechensbekämpfungsgesetz), the G-10 Law allows warrantless automated wiretaps of international communications by the Intelligence Service (BND) for purposes of preventing terrorism and illegal trade in drugs and weapons. In July 1999, the Federal Constitutional Court upheld the screening method authorized under the G-10 Law.[\[14\]](#) The Law was amended in 2001 to require that electronic communications service providers give intelligence agencies the means to monitor data as well as voice lines.[\[15\]](#) DPAs complain that after a G-10 measure any notification of the person concerned is dispensable if the data is ready for deletion.[\[16\]](#)

Direct marketing issues are addressed by Section 7 of the German Unfair Competition Act. According to its general clause, it is unfair to annoy market players, e.g., consumers, inappropriately.[\[17\]](#) By default this applies to clearly unwanted advertisements, unsolicited commercial phone calls, marketing methods making use of automated calling machines, fax machines or e-mail (spam) without prior consent, and any direct marketing that cannot be linked back to the senders' identity. Direct marketing via e-mail is not prohibited as spam under the conditions that (1) an organization has received the e-mail address in the context of selling goods or services to the customer; (2) the organization uses the e-mail contact for marketing of very similar products and services; (3) the customer has not opposed the use of his e-mail for further direct marketing; and (4) at the time of the collection and each usage of the e-mail address clearly sets out the right to opt-out from direct marketing via e-mail. Cold calling of consumers is a violation of Unfair Competition Law.[\[18\]](#)

Germany has no workplace privacy law because the Federal Government has not come up yet with a draft legislation on the subject, although the German Parliament has requested it several times.[\[19\]](#) The Federal Data Protection Officer, Peter Schaar, also cites a need for a data protection statute regarding the use of employees' personal data in the context of the monitoring of web surfing and the protection of the employers' computer systems against viruses and spam.[\[20\]](#)

Data Protection Authority

The Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz, or BfDI) is an independent federal agency that supervises the Federal Data Protection Act (BDSG) as well as the Federal Freedom of Information Act.^[21] Its chief duties include monitoring the compliance with the provisions of the BDSG by public bodies of the Federation, receiving and investigating complaints, as well as submitting recommendations to parliament and other governmental bodies. The BfDI publishes a biannual activity report.^[22] However, the number of controllers is steadily decreasing as federal agencies, in compliance with the 2001 changes to the Act, appoint in-house data protection officers, as an alternative to registration under the Act.^[23] The BfDI, which has 70 people on staff,^[24] handles about 5,516 written and oral complaints (an increase of 28%) and carries out approximately 75 investigations each year.^[25] In 2006 an amendment to the BDSG raised the threshold number of employees that make a company data protection officer mandatory from four to nine. This change has significant impact, because many small companies who were previously obligated to have a privacy officer are no longer required by statute to have one.^[26]

Wiretapping and Surveillance

Service providers are legally compelled to request the name and address of new customers to which they allocate a telephone number, even though they only use prepaid services. Telecommunications operators providing publicly available services are also mandated to provide - at their own expense - the technical facilities required to implement telecommunications interception for law enforcement purposes. The Telecommunications Interception Ordinance of January 22, 2002, which lays out specific technical requirements, remains in force until its successor will be issued under the Telecommunications Act of 2004 (TKG) by the German government. A few proposals for this law have already been circulated. However, there is still much discussion about how to include Voice over IP. Also, telephone monitoring has been on the increase since 1995, when there were 4,674 instances of monitoring, up to 35,329 in 2006.^[27] The previous figures only include those warrants that were newly issued; the total number of instances of monitoring in 2005 was 42,508.^[28] Four out of five wiretappings monitor cell phones. This renewed rise of interventions in secret communications gives the federal commissioners great concern for data security. For years, the commissioners have appealed to prosecution authorities to use this means sparingly.^[29]

As prescribed by EC Directive on Privacy and Electronic Communications, the TKG 2004 sets out the requirements of the processing of location data, either anonymously or with the subscriber's consent, for the provision of location based services.^[30] It is upon the subscriber to inform any co-users of all such consent given. In the case of "Track your Kid" services parents consent to give up their child's data protection because they are the subscribers, whereas the child is the user of the mobile phone.^[31] Apart from content, all positive and negative (e.g. the unsuccessful attempt to call) circumstances of telecommunications are protected as telecommunications privacy. Service providers are required to protect their users' personal data and telecommunications privacy. The collection and use of traffic data is strictly limited to: (1) the purposes of charging and billing, (2) remedy malfunctions in telecommunications systems, and (3) detect telecommunications service fraud and, with the consent of the data subject, (4) to market and customize services to service providers' subscribers, as well as to provide value-added services. The TKG was last amended on February 18, 2007.

The Telemedia Act (TMG) was passed in March 2007, and applies to "webshops, mobile commerce, newsgroups, music download platforms, video on demand (VOD), internet search engines, emails and even simple company websites, but not to live-streaming of

video, web-casting, IPTV (Internet Protocol TV) or VoIP (Voice Over Internet Protocol - internet telephony)."[\[32\]](#) Telemedia service providers must inform users about the "character, extent and reason" of the collection and processing of user-related data. Service providers are required under the TMG to produce user data, such as user names or addresses, upon request of the German secret services. Further, user data may be demanded if necessary for the enforcement of intellectual property rights.[\[33\]](#)

In March 2006, the EU adopted the Data Retention Directive that mandates the retention of telecommunications data for a period of 6 months to 24 months.[\[34\]](#) The implementation of the European Data Retention Directive is currently at the status of a governmental draft (Kabinettsentwurf). The draft legislation would require data retention for 6 months.[\[35\]](#) Access to retained data is given only with a warrant issued by a judge, and only if the authorities investigate a crime in the list enumerated in the proposal. However the list also covers offences not covered by the directive, such as those committed via telecommunication. This effectively will include the possibility to access the retained data also in cases of copyright violations via peer-to-peer networks. At the same time a direct access of the data by the copyright holders is discussed under the implementation of the EC law enforcement directive. The draft also aims at complying with the Cybercrime Convention. The current proposal aims at entering into force on January 1st, 2008, thus not making use of the extended implementation period for the area of internet related data the EU Directive offers.[\[36\]](#)

A significant public movement against data retention has been formed, with some thousand people attending demonstrations, and about 10,000 people declaring that they will be filing a case before the Constitutional Court, which is quite extraordinary, since the procedures do not allow for class action suits.[\[37\]](#) The Arbeitskreis Vorratsdatenspeicherung (German Working Group on Data Retention) is an association of civil rights campaigners, data protection activists and Internet users. The Arbeitskreis is coordinating the campaign against the introduction of data retention in Germany. Strong concerns on the compliance with constitutional provisions have been raised even by the scientific service of the parliament.[\[38\]](#) Prior decisions suggest that the German Constitutional Court could declare itself incompetent due to the fact that the law is necessary to comply with a European Directive.

The so-called "Grosser Lauschangriff" ("Big Eavesdropping Attack") formed part of the Law for the Enhancement of the Fight against Organized Crime, which became effective in 1999, and was intended to provide the legal basis for police to survey potential criminals. In April 1998, Article 13 of the Constitution (Grundgesetz) that provides for the inviolability of private homes was amended in order to allow police authorities to place bugging devices in private homes (provided there is a court order).

In March 2004, the German Federal Constitutional Court ruled[\[39\]](#) that significant portions of the eavesdropping Law infringed the Constitution, or Basic Law, especially Article 1 on human dignity and Article 13 on the inviolability of private homes.[\[40\]](#) The court held that certain communications are protected by an absolute area of intimacy wherein citizens can communicate privately without fear of government surveillance.[\[41\]](#) This includes conversations with close family members, priests, doctors and defense attorneys, but excludes conversations about crimes that have already been committed or the planning of future crimes. However, to justify surveillance between the target and such persons of trust, the government must show that "there is strong reason to believe that the content of conversation does not fall in the area of intimacy,"[\[42\]](#) and that the crime is "particularly serious."[\[43\]](#) Once a specially protected conversation begins, the eavesdropping must stop immediately and any recordings of that portion of the conversation must be erased. The German legislature was granted a transitional period until June 2005 to comply with the court's decision, and in May 2005 the German Bundestag passed legislation to comply with the court.[\[44\]](#)

In 2001, the Bundestag (the German Parliament) passed a law that added to the Criminal Procedural Code (StPO) further means of investigation into electronic communications. It serves as the legal basis for police and law enforcement to access "telecommunications connection data" for the investigation of serious crimes. The law took effect in January 2002 and requires telecommunications service providers to disclose data, such as time and duration of use, place of use and identifying numbers.[\[45\]](#) The report is not yet available.[\[46\]](#) In October 2004, the Parliament extended its application until January 1, 2008, together with a request to the Federal Government (Bundesregierung) for a detailed report until June 30, 2007, containing causes, results and the exact number of measures taken under this law.[\[47\]](#) According to a survey, 75 percent of conducted telephone wiretapping actions violated the law. In most instances of wiretapping, law enforcement agencies did not inform the subjects after the eavesdropping took place, contrary to what is stipulated by the law.[\[48\]](#)

In 2004, a new regulation of the German Criminal Code (§201a StGB) took effect. This regulation protects private life against the invasion of privacy by the taking of pictures of persons in their apartments or other protected areas, e.g., changing cabins. Furthermore, publishing and distribution of such photographs on the Internet is punishable as a criminal offense.

In April 1998, a law was passed that allows the Bundeskriminalamt (Federal Police) to run a nationwide database of genetic profiles related to criminal investigations and convicted offenders. One month later, the Bundespolizei (Border Protection Forces), originally a paramilitary border police force but now responsible for securing and controlling borders, as well as working in foreign embassies, received permission to check persons' identities and baggage without any concrete suspicion.[\[49\]](#)

Location Privacy

Germany also implemented in the StPO the possibility of using a so-called IMSI-Catcher system to track individuals through the location of their cell phones. The law, which entered into force on August 14, 2002, provides law enforcement with the ability to obtain, upon court request and from the time it is granted, the data of individuals' movements and their cell phone device number (IMEI number - International Mobile Equipment Identity) for a period of up to six months.[\[50\]](#) The location of a mobile phone can further be conducted with silent SMS that is covered by general investigation powers in criminal cases.[\[51\]](#) Silent SMS means that an empty message is sent to a mobile phone, which allows for some approximation of its whereabouts, but it does not report itself to the respective user.

The Federal Constitutional Court (Bundesverfassungsgericht) has ruled that the police may use GPS technology to track suspects driving motor vehicles in cases of serious crimes even without a judicial warrant.[\[52\]](#) The Court approved §100c StPO to be consistent with the Constitutional principle of clarity and definiteness and when allowing police to use "all technical observational means" to investigate suspicious behaviour that might be considered a crime of substantial significance. However, the Court stressed that Parliament had to monitor the fast technological developments in this field and may have to correct laws if the risks for fundamental rights caused by technical surveillance increase. Parliament also has to ensure by procedural rules that law enforcement agencies (e.g. from different Länder or the Federal level) do not subject citizens to uncoordinated surveillance measures. The "additive effect" on fundamental rights has to be kept in mind.

In 2005, a new system to electronically collect tolls for trucks using the national highways was launched. The system tracks vehicles through GPS (Global Positioning System) and cellular phone networks. According to a common standpoint of the DPAs in 2001, the Federal government implemented special data protection measures in the laws governing toll systems: data collection and processing is limited only for the purpose of billing; all

data must be deleted after the payment; and all data collected from vehicles that are not subject to a toll must be immediately deleted.[\[53\]](#) After a series of murders allegedly committed by the same offender, there are now plans by the government to abolish these restrictions.[\[54\]](#) If law enforcement could have access to the data, the movement of almost all cars and trucks on German highways could be monitored.

German authorities have also recently proposed implementation of a video surveillance system at toll collection points, to ensure that trucks from other countries are paying the proper tolls on the autobahn.[\[55\]](#) Video footage would be compared against a central database. Privacy and data security groups have protested this proposal, citing the possibility for using the data for purposes other than toll-collection. Indeed, although this surveillance data is only supposed to be used for toll-collection and enforcement purposes, the German police recently gained access to the data when trying to locate a stolen garbage truck.[\[56\]](#) The Federal Government (Bundesregierung) recently stated that it is not aware of any access by law enforcement to information of the toll system.[\[57\]](#) Independently from the toll system, in the State of Hessen the new Police Law of December 2004 permits the electronic scanning of vehicles' number plates that are then automatically matched with a database of searched vehicles.[\[58\]](#)

There are several other video surveillance projects in Germany that have generated a response from privacy and data protection advocacy groups. For example, a private group called Der Grosse Bruder (Big Brother)[\[59\]](#) has created a map of Munich, highlighting all the video surveillance cameras installed there.[\[60\]](#) In 2003, the Humanistische Union (Humanistic Union)[\[61\]](#) sued a Berlin shopping center employing a video surveillance system with a range of vision that included a public street.[\[62\]](#) In Weimar, Germany, a local newspaper protested the installation of video surveillance cameras that watched the entrance of a newspaper building (along with medical and political offices), and the local government eventually uninstalled the cameras.[\[63\]](#) Public debate on camera observation was heightened by the revelation that a museum's security camera could see into chancellor Angela Merkel's private flat in Berlin. Upon discovery, the mechanism of the camera was changed to reduce the angle of observation.[\[64\]](#)

RFID

In May 2003, the German retail giant Metro started a trial project to introduce a new cashing and customer convenience program with small chips, called Radio Frequency Identification (RFID) chips, at their Metro Future Store. The chips will be attached to all products. When queried by a radio device, RFID chips respond by transmitting a unique ID code. It therefore allows customers to pay and checkout automatically by pushing a loaded trolley past a sensor. Combined with an automatically readable customer client card, the system would allow the tracking of all purchases and the linking to the customer's identity.[\[65\]](#) Metro claimed that the RFID chips could easily be deactivated, thus erasing any privacy invasions, but their process for deactivation leaves intact the unique identifying number on the RFID chip, so even "deactivated" cards can be traced back to their origin.[\[66\]](#) In March, 2004, Metro halted the trial program in response to protests from digital rights groups regarding possible privacy violations.[\[67\]](#) Outcry was particularly forceful upon discovery that Metro had placed RFID devices in their "Extra Future Card" (personal customer shopping card) without notifying consumers.[\[68\]](#) This use of RFID was uncovered by a German NGO called FoeBuD by taking X-ray photos of the card.[\[69\]](#) FoeBuD also staged two protests, one in front of the Metro Future Store and one at a "pro-RFID" conference, and has recently been granted money by the Bewegungsstiftung[\[70\]](#) (a German group which supports and promotes social movements and reform projects) to develop the "privatizer," a small device which consumers could use to find hidden and embedded RFID chips in consumer products.[\[71\]](#) In a recent speech, the Federal Data Protection Commissioner pointed out the privacy implications of RFID, and called on the legislature to make provisions on RFID tags.[\[72\]](#)

RFID-chipped tickets for the 2006 Football World Cup in Germany enabled authorities to track the movements of the individualized spectator during the event. [73] The application forms for tickets required a large number of personal information, i.e. passport number, nationality, and day of birth. This was subsequently upheld by the courts. [74]

Biometrics

Germany was among the first states in the EU to introduce the new biometric passports, following the EU Council Regulation on standards for security features and biometrics in passports and travel documents issued by the Member States. [75] Since November 1, 2005, the German passports contain RFID chips with facial images, and beginning November 1, 2007, the chips will also include fingerprints. After much debate between the ruling coalition parties (Social Democrats and Christian Democrats), it was decided to store the fingerprint data neither in a central nor in local databases. Subsequent to the production of the passport, the manufacturer and local authorities are obliged to delete the data. Furthermore, this also applies after every verification process. Apart from the short-term processing of the data in specific control situations, the fingerprints are thus only to be stored in the German passport itself and not in any databases of public authorities.

The Federal Labour Court (Bundesarbeitsgericht) ruled that the use of biometrics at entrance controls of workplaces is subject to compulsory employee participation (Mitbestimmung) and thus only legal after approval of the respective workers' council or arbitration board. [76] Importantly, this also applies if the biometric system is placed at the premises of a third party (e.g. the customer of a service company), when the employer instructs his/her employees to use the system.

Open Government

On January 1, 2006, the Federal Freedom of Information (FOI) Act entered into force, [77] thereby closing the gap in transparency between Germany and all other Member States of the European Union (except Cyprus, Luxembourg, and Malta). FOI legislation had been proposed for five years but the administration had been reluctant to agree on a draft statute. Eventually, Members of Parliament from the ruling coalition parties grew impatient for a draft and presented their own. [78] The draft was followed by an intense debate in the German Parliament (Bundestag) and among legal scholars that particularly focused on the exceptions included in the Act. Much criticism focused on the fact that information can be rather easily excluded from disclosure on grounds of public security and fiscal interests of the government. Personal data will only be disclosed if the information interest outweighs the interest of the data subject. Importantly, information containing intellectual property or business secrets is completely excluded from the ambit of the Act. The Federal Commissioner for Data Protection and Freedom of Information enforces the FOIA Act. [79]

Eight of the Länder already have their own FOI laws in effect. [80] The Land of Brandenburg has the right of access to governmental records in its constitution and adopted a FOI law in 1998. [81] Later, Berlin, Schleswig-Holstein, and Nordrhein-Westfalen, Hamburg, Bremen, Mecklenburg-Vorpommern, and Saarland also adopted FOI laws.

International Obligations

Germany is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108) [82] and later signed an Additional Protocol to this convention. [83] It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (Convention No. 005). [84] In November 2002, Germany signed the Convention on Cybercrime but has not yet ratified it. [85] It is a member of the

Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[1] Available at [\[link\]](#) (in German).

[2] Federal Constitutional Court (Bundesverfassungsgericht) decision of December 15, 1983, reference number: 1 BvR 209, 269, 362, 420, 440, 484/83.

[3] Federal Act on Data Protection ("BDSG"), January 14, 2003, last amended on November 15, 2006 (Bundesgesetzblatt, Part I, No 3, January 16, 2003, last amended on November 15, 2006), available at [\[link\]](#).

[4] German Parliament (Bundestag) decision of February 17, 2005, available at [\[link\]](#); Response of the Federal Government from January 26, 2005 to the questionnaire of the Parliament, available at [\[link\]](#) (in German).

[5] See Modernisierung des Datenschutzes: Öffentliche Anhörung des Innenausschusses (Modernization of the data security: Public hearing of the interior committee), March 6, 2007, available at [\[link\]](#) (in German).

[6] English summary available at [\[link\]](#); Full version available at [\[link\]](#) (in German).

[7] Id.

[8] Id.

[9] German Parliament (Bundestag) decision of February 17, 2005, available at [\[link\]](#).

[10] Complete text in German available [\[link\]](#); [\[link\]](#); [\[link\]](#).

[11] Landesbeauftragte für den Datenschutz (the Representatives of the Länder's data protection authorities), available at [\[link\]](#).

[12] See for a complete list of documents [\[link\]](#) (in German).

[13] Available at [\[link\]](#) (in German).

[14] Federal Constitutional Court (Bundesverfassungsgericht), decision of July 14, 1999, reference numbers: 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95.

[15] "Germany: New Law Allows More Extensive Government Monitoring of Phone Calls and Email," World Socialist Web Site, February 20, 2001.

[16] 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Düsseldorf, 8.-9.05.2001." available at [\[link\]](#) in German.

[17] German Unfair Competition Act, available at [\[link\]](#) (in German).

[18] Id.

[19] Response of the Federal Government from January 26, 2005 to the questionnaire of the Parliament, available at [\[link\]](#) (in German).

[20] Peter Schaar also questions proposals to reform the Electronic Signature Statute, which the Parliament wants to change to require all certification centers to disclose the identity of all signature key owners to law enforcement, intelligence, or tax agencies upon request. The law as it stands merely stipulates the disclosure in cases where the signature owner is using a pseudonym. Peter Schaar, *supra*.

[21] German Parliament Decision of September 5, 2005, available at [\[link\]](#). Homepage [\[link\]](#); English description of the duties of the Federal Data Protection Commissioner available at [\[link\]](#).

[22] "20. Tätigkeitsbericht 2003/ 2004," available at [\[link\]](#).

[23] E-mail from Ulrich Dammann, Bundesbeauftragte für den Datenschutz, to Christian Schröder, Law Clerk, Electronic Privacy Information Center, April 4, 2003 (on file with EPIC).

[24] [\[link\]](#).

[25] BfDI, Tätigkeitsbericht (Bi-Annual Report) 2005-2006, April 24, 2007 at 160, available at [\[link\]](#).

[26] German Parliament Decision of August 22nd, 2006, available at [\[link\]](#).

[27] "Telefonüberwachung: Keine Steigerung in 2006", Bundesnetzagentur, Press Release of Februar 26th, 2007, available at [\[link\]](#) (in German).

[28] "Überwachung der Telekommunikation hat erneut zugenommen", heise online, October 19th, 2006, available at [\[link\]](#).

[29] Press information 12/05 of the Federal Data Protection Commissioner (Bundesdatenschutzbeauftragter) of March 31, 2005, "Telefonüberwachungen auch 2004 wieder stark gestiegen".

[30] Telecommunications Act 2004, available at [\[link\]](#).

[31] Response of the German government (Bundesregierung) of January 26, 2005, to parliamentary question, reference number (Drucksache) 15/4725.

[32] Henning Kreig, "German Telemedia Act introduces new rules for New Media," Bird & Bird Articles, March 5, 2007, available at [\[link\]](#).

[33] Id.

[34] [\[link\]](#).

[35] EDRI-Gram, Number 5.8, April 2007, available at [\[link\]](#).

[36] "Stellungnahme zum Regierungsentwurf für eine Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" of June 20th, 2007, available at [\[link\]](#).

[37] [\[link\]](#).

[38] "Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht", Scientific Services of the German Parliament of August 8th, 2006, available at [\[link\]](#).

[39] Federal Constitutional Court (Bundesverfassungsgericht) decision of March 3, 2004, reference number: 1 BvR 2378/98, available at [\[link\]](#) (in German).

[40] Basic Law for the Federal Republic of Germany, I. Basic Rights, Articles 1, 13, available at [\[link\]](#).

[41] C. Schröder, "Wiretap in Germany," German American Law Journal: American Edition (March 11, 2004), available at [\[link\]](#).

[42] Id.

[43] University College of London, Faculty of Laws, Institute of Global Law, "German Legal News - Constitutional Law," available at [\[link\]](#).

[44] "Änderungen beim großen Lauschangriff", Das Parlament, Nr. 20 of May 17th, 2005, available at [\[link\]](#).

[45] Federal Bulletin, BGBl I 2001, 3879, available at [\[link\]](#) (in German).

[46] Email from Jan Schallaböck, Unabhängiges Landeszentrum für Datenschutz, Germany, to Allison Knight, Research Director, Electronic Privacy Information Center, June 21, 2007 (on file with EPIC).

[47] Decision of the Parliament (Bundestag) of October 21, 2004, reference number 15/3349, 3971, available at [\[link\]](#) (in German).

[48] "Dreiviertel aller Lauschangriffe rechtswidrig," Der Spiegel Online, January 9, 2003, available at [\[link\]](#) (in German).

[49] "New Powers for the Border Police: Checks Anywhere at Any Time," Fortress Europe, FECL 56 (December 1998).

[50] 19. Tätigkeitsbericht - 2001/2002 at 54-55, available at [\[link\]](#) (in German).

[51] Response of the Federal Government from January 26, 2005 to the questionnaire of the Parliament, available at [\[link\]](#) (in German).

[52] Federal Constitutional Court (BVerfG), decision of April 12, 2005, reference number 2 BvR 581/01, available at [\[link\]](#) (in German).

[53] Gesetz zur Änderung des Fernstrassenbauprivatisierungsgesetzes, BGBl. I 2002 Nr. 63, 3442, available at [\[link\]](#); Response of the Federal Government from January 26, 2005 to the questionnaire of the Parliament, available at [\[link\]](#) (in German).

[54] [\[link\]](#).

[55] E-mail from Bettina Winsemann, Staff Member, STOP1984, to the Electronic Privacy Information Center, July 9, 2004 (on file with EPIC).

[56] Christiane Schulzki-Haddouti, "Fahnder wollen Daten aus LKW-Mautsystem" (Investigators Want Data from Truck Mautsystem), Heise online, October 31, 2003, available at [\[link\]](#) (in German).

[57] Response of the Federal Government from January 26, 2005 to the questionnaire of the Parliament, available at [\[link\]](#) (in German), at 30 (in German).

[58] Heise News of December 15, 2004, "Hessen dehnt Polizeibefugnisse deutlich aus," available at [\[link\]](#) (in German).

Page 56 to 73

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- [59] Homepage at [\[link\]](#).
- [60] Munich Atlas at [\[link\]](#).
- [61] Homepage at [\[link\]](#).
- [62] Stefan Krempf, "Urteil schränkt Videüberwachung ein" ("Judgement Limits Video Monitoring"), Heise online, December 12, 2003, available at [\[link\]](#) (in German).
- [63] Peter Nowak, "Weimarer Provinzposse mit Kamera," Telepolis, October 27, 2003, available at [\[link\]](#) (in German).
- [64] "Wachleute filmten heimlich Merkels Wohnzimmer", Spiegel online of Mach 26th, 2006, available at [\[link\]](#) (in German).
- [65] "Retail Future: Painless Checkout, Knowing Scanners," Reuters, May 14, 2003 [\[link\]](#).
- [66] E-mail from Bettina Winsemann, Staff Member, STOP1984, to EPIC, July 12, 2004.
- [67] "German Revolt Against RFID", The Register, March 1, 2004, available at [\[link\]](#).
- [68] See FoeBuD, RFID web page at [\[link\]](#); Under § 6(c) of the BDSG, notice must be provided to data subjects of communications with "intelligent" RFID (devices with integrated processors), thus prohibiting secret reading or writing of personal information. However, Germany does not yet have any regulations specifically addressing "non-intelligent" RFID, which still create a privacy risk, as they can be linked to personal information held elsewhere without violating § 6(c). (E-mail from Christian Schröder, former Law Clerk with EPIC, June 18, 2004 (on file with EPIC).)
- [69] FoeBuD, RFID web page available at [\[link\]](#).
- [70] Bewegungsstiftung [\[link\]](#).
- [71] E-mail from Bettina Winsemann, Staff Member, STOP1984, to EPIC, July 12, 2004 (on file with EPIC); See also "Funkchip-Kontrolle für Konsumenten" (Radio Chip Control for Consumers) [\[link\]](#).
- [72] Peter Schaar (Federal Data Protection Commissioner), "Datenschutz als Verbraucherschutz: Neue Herausforderungen am Beispiel von Smart Chips und Kundenkarten," April 5, 2004, available at [\[link\]](#).
- [73] Monika Ermert, "World Cup 2006 'Abused for Mega-surveillance Project', The Register of February 8, 2005, available at [\[link\]](#).
- [74] Decision of September 1, 2006, 2-01 S 111/06.
- [75] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal 2004 L 385, p.1.
- [76] 1 ABR 7/03, January 24, 2004, available at [\[link\]](#) (in German).
- [77] Available at [\[link\]](#) (in German).
- [78] Draft of a federal Freedom of Information Law, available at [\[link\]](#) (in German) and [\[link\]](#) (in English).
- [79] German Parliament Decision of September 5, 2005 [\[link\]](#).
- [80] See for an overview [\[link\]](#).
- [81] FOI Brandenburg (Akteneinsichts- und Informationszugangsgesetz ("AIG"), 1998), available at [\[link\]](#) (in German).
- [82] Council of Europe, Legal Affairs, Treaty Office at [\[link\]](#).
- [83] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, available at [\[link\]](#).
- [84] Council of Europe, Legal Affairs, Treaty Office at [\[link\]](#).
- [85] Council of Europe, Convention on Cybercrime, available at [\[link\]](#).
<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559535>

ANNEX 8:

Note for retailer concerning a model contract for issuing an e-ticket-chipcard (Germany)

This document has been provided after a workshop at VDV Cologne on November 18, 2009.

The customer has to be informed that he can decide between either an anonymous participation in the ((eTicket Deutschland (Germany)), or a participation by using PT via payment made by direct debit respectively credit card, or by means of an automatic charging process.

If the customer decides to use an anonymous entitlement for payment, he gets a voucher including the relevant data of the customer contract (entitlement_identification, validity, means of payment), instead of a individual-related customer contract form.

Therefore the following model contract form is only used for individual-related entitlements concerning the means of payment of the ((eTicket Deutschland (Germany)).

Application form for issuing an e-ticket-chipcard (user medium) of [xy] transport companies Ltd. (GmbH)

Terms and conditions for user media of xy transport companies Ltd. (GmbH)

A. General rules

The rules made in paragraph A are valid for all e-ticket smartcards („user medium“) issued by [xy] transport operators Ltd. GmbH, [ADDRESS] („Company“). ((eTicket Deutschland is offered as a modern, fast, and secure alternative to the furthermore existing use of a paper ticket.

1. Applicability

The [xy] smartcard („user medium“) is issued by the company. According to the following rules the owner („user“ or traveller or passenger or customer) of the e-ticket smartcard is allowed:

- to store electronic tickets for transport services of VDV-EFM-contracting companies in the user medium,
- to make use of transport services of VDV-EFM contracting companies via automatic entitlements stored in the user medium and
- to pay cashless for entitlements of VDV-EFM contracting companies (paper tickets, electronic tickets, automatic entitlements). By arrangement, payment is carried out either from a debit charged on the user medium („payment feature debit prepaid anonymously or debit prepaid with autoload function“) or postpaid by direct debit of the sales made via user medium, which the company paid by means of direct debit from the account named to it by the user, by order and for account of the user („payment feature: postpaid“) in Germany.

The user medium can be used without identification features. The identification features mentioned under cypher A.3. are only meant for the usage of several service functions.

VDV-EFM contracting companies, acceptance points and acceptance terminals, charging points and charging terminals, referred to in this terms and conditions, can be identified by the acceptance symbols stamped on the user medium.

2. Entitlements

2.1 Electronic ticket („EFS“)

According to the respectively effective terms of transportation and tariff provisions the user can make use of transportation services for certain VDV-EFM contractual companies, which can be stored in the user medium. VDV-EFM contracting companies, accepting EFS, can be identified by the acceptance symbols stamped on the user medium.

2.2. Automated Fare Collection („AFB“)

The user possesses an automated fare collection entitlement stored in the user medium with which he can make use of transportation services of certain VDV-EFM contracting companies according to their respectively effective terms of transportation and tariff provisions, without separately buying another entitlement. VDV-EFM contracting companies, accepting automated fare collection (AFB, can be identified by the acceptance symbols stamped on the user medium.

The collection of the transportation services used occurs either because the user simply carries the user medium with himself, or because he directs it to a contactless measuring device - depending on the collection method used by the VDV-EFM contracting company. The VDV-EFM contracting company advises the customer conveniently, which collection method will be used.

Transportation services via automated fare collection (AFB) stored in the user medium can not be used, if the automated fare collection (AFB) stored in the user medium is blocked. This will be especially the case if the payment feature stored in the user medium is blocked.

2.3. Parallel use of AFB and EFS

Unless one or several valid electronic tickets are stored in a user medium which includes an AFB, first of all the valid electronic tickets will be accessed for using the transportation services of the VDV-EFM contracting company. As far as the valid electronic tickets stored in the user medium are insufficient for the payment of the used transportation service, the payment will be made based on the valid AFB.

3. Means of identification

The company provides the user with several means of identification (e.g. identification number, PIN, Login and password for access to the Net) which are required for several service functions. The user will be informed of the right usage of the means of identification separately. The user has to ensure that no other person knows his means of identification. **Each other person who knows the means of identification is able to misuse it.**

4. Fees

4.1. Amount of the fees

The company is authorised to bill the user for the services performed in connection with the contract conceding the issuance of the user medium („user medium contract“). The amount of the fees results from the particularly valid price list at the specific date.

4.2. Change of fees

The company is authorized to change the fees at its own discretion (§ 315 German Civil Code). It will inform the user of the changes. In case of an increase of the fees, the user is allowed to withdraw from the user medium contract within six weeks with immediate effect after the official announcement of the changes. If the user withdraws from the contract, the increased fees will not be taken into account for the terminated user medium contract.

5. Duty of care and other obligations of the user

5.1. Safekeeping of the user medium

The user has to keep his user medium safe, in order to avoid fraud. As long as the user medium has not been blocked, each Person who is able to get the user medium, is also able to use the electronic tickets stored in the user medium and/or to pay with the user medium without using the means of identification.

5.2 Obligations in case of loss or fraud

As soon as the user discovers that he has lost his user medium or that another person misused it, the user is obligated to inform the company [ADDRESS, PHONE) in order to block the user medium. After the company has been informed about the loss of the user medium, it will block the user medium. In case of fraud, the user has also to report an offence to the police.

5.3 Obligations in case of malfunction of the user medium

In case of damage, the user has to buy a conventional alternative ticket before he starts his trip. Thereafter he is obligated to contact the company for trouble shooting. The company reimburses the amount for the alternative ticket, if the user is not to blame for the damage of the user medium.

5.4 Duty of notification in case of change of personal data

The user is obligated to inform the company about every change concerning his personal data as well as every change concerning his banking account. The user has to take over the accruing costs for every breach of this duty.

6. Reimbursement of the electronic ticket (EFS) in case of loss of the user medium

In case of loss of the user medium, the user is not eligible for compensation of the EFS, stored in the user medium, by the service provider. Possible claims for damages against the VDV-EFM contracting company which sold the electronic tickets to the user, depend on the applicable terms of transportation and tariff.

7. Ownership and validity of the user medium

7.1. Ownership

The user medium remains property of the company.

7.2. Validity

The validity of the user medium is stamped on it. Getting a new user medium, at the latest when the user medium is no longer valid, the user is obligated to give the user medium back to the company. The valid electronic tickets and the deposit still stored in the user medium will be assigned to the new user medium.

8. Right of termination of the user

The user can terminate the user medium contract without notice at any time.

9. Right of termination of the company

9.1. Proper notice of termination

The company can terminate the user medium contract with an at least six weeks' notice. The company will terminate the user medium contract with a longer term of notice, as far as the interests of the user demand.

9.2. Termination for cause without term of notice

The company is allowed to terminate the user medium contract without notice for cause. An important reason is, especially:

- that the user does not come up to the duty of payment stated in the contract, within an appropriate period set by the company,
- that the user manipulates the user medium in order to misuse it,
- that the user damages or destroys the user medium planned in advance or negligent, or
- that the user offends against any duties from the user medium contract.

10. Consequences of the termination of the user medium contract

10.1 Expiration of the entitlement to use and obligation to return the user mediums

By entry into force of the termination or in case of abnormal termination of the user medium contract („termination of the user medium contract“), the user is not longer allowed to use the user medium. He is obligated to give it back to the company unrequested and as soon as possible.

10.2 Reimbursement of stored electronic tickets (EFS)

The valid electronic tickets still stored in the user medium when the user returns the user medium to the VDV-EFM contracting company where he has bought the particular electronic tickets will be reimbursed according to the applicable terms of transportation and tariff. There exists no claim for reimbursement against the company from this business relation.

10.3 Reimbursement of the residual deposit

The user is allowed to chose, whether the deposit stored in the user medium shall be reimbursed in cash or at a bank account named by the user.

10.4 Instantaneous due for settlement of the claims of the company

According to the contractual relationship all demands of the company against the user become due immediately, by ending of the user medium contract.

11. Blocking and retraction of the user medium, consequences of the collection

11.1 Blocking and retraction

The company is allowed to block the user medium either completely or for several applicabilities as described in cypher A. 1. and/or to collect the user medium in case the user medium contract is terminated for cause.

The company is even then allowed to block or to collect the user medium, when the entitlement to use the user medium ends because of the ending of the user medium contract or because of the end of validity of the user medium.

11.2 Consequences of retraction because of end of validity period

Will the user medium be collected because of the end of validity, the directed legal consequence in cypher A.10.2 and cypher A.10.3. applies accordingly, regarding the electronic tickets and the deposit stored in the user medium.

11.3 Consequences of retraction for other reasons

Will the user medium be collected because of other reasons, according to cypher A.11.1., the directed legal consequences in cypher A.10.2 and cypher A.10.3. apply accordingly, regarding the electronic tickets and the deposit stored in the user medium.

12. Changes or supplements of the terms and conditions

The user will be informed about changes or supplements to these business conditions in written form. If the user does not file an objection in written form within six weeks after

official announcement of the changes or supplements, they are regarded as accepted by the user. The company will advise the user of this consequence explicitly. The date of the postmark is important for the timeliness of the objection.

13. Applicable law, place of jurisdiction

13.1 Applies according to German law

This contract is subject of the law of the Federal Republic of Germany.

13.2 Place of jurisdiction

If the user is a merchant, a body corporate under public law or a special property governed by public law, the company is only allowed to take an action at its place of general jurisdiction and it can also only be brought an action against it at this place of jurisdiction.

14. Information concerning bank account

Hereby the user authorises his bank to provide the company, respectively the bank assigned by the company, with the necessary information concerning the issuance or maintenance of the user medium. **This means exclusively the information that the user in fact is owner of a bank account at the bank stated by him. Information concerning credit-rating is excluded.**

B. User media with payment feature: postpaid

The arrangements made in paragraph B. are valid for the usage of user media with the payment feature: postpaid.

1. Payment of entitlements

1.1. Payment of electronic tickets (EFS) and paper tickets

Electronic tickets and paper tickets can be paid cashless at the acceptance points and acceptance terminals via the payment feature „postpaid“.

1.2. Payment in case of Automated Fare Collection (AFB)

In case of using AFB, cashless payment via payment feature “postpaid” results from the fact that the user either simply carries the user medium with himself, or because he directs it to a contactless measuring device - depending on the collection method used by the VDV-EFM contracting company. The VDV-EFM contracting company advises the customer conveniently, which collection method will be used.

2. Claim for reimbursement of the company, billing of the sales, blocking

2.1. Claim for reimbursement of the company

The user instructs and authorises the company irrevocably to settle the bills outstanding from the VDV-EFM contracting companies, for either own use of his user medium or for the use by a third party he authorised to make use of his user medium. The user is obligated to reimburse the company all emerging expenses.

2.2 Billing of the sales

At the end of the agreed accounting period the user gets a bill for all sales made for transportation services with his user medium within the particular period. The amount stated in the bill falls due for payment immediately and will be directly debited by the company from the account of the user. For this purpose the user has to name a bank account at a domestic bank.

2.3. Verification of billing, acceptance of billing

The user is obligated to make sure that the bills are accurate and complete. Possible objections have to be notified to the company in written form at the latest six weeks after receipt. Here a distribution within the time limit is sufficient. If user does not object the bill on time, the bill is classified as accepted. The company will advise the user of this consequence explicitly. The user is allowed to demand a correction of the bill, even after expiration of the deadline. In this case he has to verify that the bill is not correct or incomplete.

2.4 Blocking of the payment feature postpaid due to the return of a direct debit

The user is obligated to assure that his account is in credit with a sufficient amount for the sales made with the user medium, when the company debits his account. If the direct debit can not be executed because the account is not covered, or rejected with the notice „account closed“ because of unjustified revocation made by the user, the company is authorised to block the payment function postpaid. The user has to pay for the emerging costs. In this case a termination for cause according to cypher A.9.2. remains unaffected.

3. Liability for damages caused by fraud

3.1 Liability for damages after loss of the user medium

From the moment the user informed the company about the loss of his user medium, he is no longer responsible for fraudulent use of his user medium at a later date.

3.2 Liability for damages caused before notice of loss

In case damages caused by fraudulent use of the user medium occurs before the user informed the company, his liability is limited up to 150 €, unless he caused the fraudulent use with intent or grossly negligent. In this case the user is absolutely liable for the full amount. The user's acts are grossly negligent especially if he does not inform the company immediately after he noticed the loss, or if he did not keep the user medium carefully in order to avoid fraud.

C. User media with payment feature: prepaid

The arrangements made in paragraph C. are valid for the usage of user media with the payment feature: prepaid.

1. Payment of entitlements

1.1 Payment of electronic tickets (EFS) and paper tickets

Electronic tickets and paper tickets can be paid cashless at the acceptance points and acceptance terminals via the payment feature „prepaid“.

1.2 Payment in case of Automated Fare Collection (AFB)

In case of using AFB, cashless payment via payment feature „postpaid“ results from the fact that the user either simply carries the user medium with himself, or because he directs it to a contactless measuring device - depending on the collection method used by the VDV-EFM contracting company. The VDV-EFM contracting company advises the customer conveniently, which collection method will be used.

1.3 Usage of the user medium within the amount of money charged in the medium

The payment for the sales made with the user medium is effected by the amount of money charged in the user medium. The user is only authorised to use his medium if the payment for the sales is guaranteed.

2. Charge of the user medium, maximum amount of charging, available limit per legal year

2.1 Charging with cash or cashless

The user can charge his user medium with cash or cashless at any charging point or charging terminal. An anonymously participation in the payment method prepaid can only be accepted in cash.

2.2 Charging via autoloading function

A user medium with the payment feature prepaid with autoloading function will be charged automatically with the amount agreed upon between user and company when there is either no more money on the user medium, or when the amount of money has fallen below a certain sum. The amount charged in the user medium will be debited directly against a bank account named by the user. For this purpose the user has to name a bank account at a domestic bank. Normally, the autoloading function will take up to four business days. By force of unexpected circumstance it could even take more time.

The user is obligated to assure that his account is in credit with a sufficient amount for the autoloading transaction. If the direct debit for the autoloading transaction is rejected for whatever reasons, the company is authorised to block the autoloading function. The user will be informed about the blocking of the autoloading function. The user is obligated to reimburse the company all emerging expenses.

2.3 Maximum amount of charging

The user medium can be charged up to a maximum amount of 150 €.

2.4 Available limit per legal year

In case the user did not fill in his personal data in the company's „application form for issuing an e-ticket-chipcard“, he is authorized to process payments up to an amount of 2.500 € via the payment feature „prepaid“ per legal year. When this amount has been reached, the user medium can not be charged any longer, unless, the user discloses his personal data by means of an application form for issuing an e-ticket-chipcard“.

3. Blocking of the payment feature prepaid

The company is authorised to block the payment feature „prepaid“ if the user uses his medium although there is not enough money charged in the user medium to pay for his sales. In this case a termination for cause according to cypher A.9.2. remains unaffected.

A blocking of the payment feature „prepaid“ by the company is also allowed if the available limit has been reached in terms of cypher 2.4.

4. Encashing of prepaid deposit

At any time the user can encash his deposit charged in the user medium partially or completely. As requested by the customer, the deposit charged will either be paid cash or it will be transferred into a bank account named by the user. The company will bill the user only for the costs accruing from the procedure of encashing.

5. Liability for damages caused by fraud

5.1 Liability for damages caused after notice of loss

From the moment the user informed the company about the loss of his user medium, he is no longer responsible for fraudulent use of his user medium at a later date.

5.2 Liability for damages caused before notice of loss

In case damages caused by fraudulent use of the user medium occurs before the user informed the company, his liability is limited up to 150 €, unless he caused the fraudulent use with intent or grossly negligent. In this case the user is absolutely liable for the full amount. The user's acts are grossly negligent especially if he does not inform the company immediately after he noticed the loss, or if he did not keep the user medium carefully in order to avoid fraud.

ANNEX 9:

Berliner Beauftragter für Datenschutz und Informationsfreiheit (An der Urania 4-10, 10787 Berlin)

VDV-Kernapplikations GmbH & Co. KG
 Kamekestr. 37-39
 50672 Köln

46.305.1

Joint data protection standards for electronic fare management

Delegates at the 64th Conference of Data Protection Officers of the Federal and State Government held on 24-25 October 2002 in Trier unanimously acknowledged the paper presented by the state data protection officer of North-Rhine Westphalia [LfD = Landesbeauftragte für den Datenschutz], which had been agreed on at a work group on "basic requirements in terms of data protection" for Electronic Fare Management (EFM).

At a meeting of the work group VDV [Verband Deutscher Verkehrsunternehmen = Association of German Transport Companies] with representatives of data protection officers and regulatory authorities held on 30 June 2008, the representatives of the data protection authorities were informed as to how these basic requirements have been or will be taken into account in VDV-Core Application's specifications for electronic fare management as the basic standard for an eTicket Germany.

During a coordination discussion held on 19 August 2008 at the BlnBDI [Berliner Beauftragter für Datenschutz und Informationsfreiheit= state data protection officer of Berlin], which was originally to have served as the data protection accompaniment for the extension of the EFM in Europe, the representatives of the VDV-Kernapplikations GmbH und Co. KG expressed the wish that the joint data protection standards should be formulated for all transport companies intending to use the Core Application.

As a first step, the basic requirements in terms of data protection will be set out here in tabular form and compared with the measures necessary for their implementation.

<p>1. Transparency</p> <p>Data processing via the EFM must be transparent (Section 6 c Para 1 No. 2 and 3 BDSG = Bundesdatenschutzgesetz [Federal Data Protection Act]).</p> <p>This requires</p> <ul style="list-style-type: none"> * Determination of purposes. * Description of the individual 	<p>An information document (see the attached data protection notification) describing the data processing operations and the data which is stored in the user-medium (chip card) must be provided. This document is made available by the customer contract partner</p>
---	---

<p>data processing operations distinguished according to business process relevant for the passenger and the data to be processed in this regard.</p> <ul style="list-style-type: none"> * Information on the identity and addresses of those authorities who process personal data for the aforementioned purposes and/or through whom relevant legal claims can be asserted and process descriptions can be inspected according to Section 4g Para 2 Sentence 2 BDSG. * Inclusion of the customer contract partner's information obligations. A leaflet or information sheet should be drawn up for this purpose to inform the passenger in a generally understandable way of the intended data processing - also through central service points or other authorised third parties - and of his rights according to Sections 34, 35 BDSG. 	<p>(retailer). Important contents of this information paper are included in the so-called customer interface specifications, which is an integral part of the KA specifications and EFM participation contracts to be adhered to by the participating companies.</p> <p>In addition, in connection with the "application to issue an eTicket (user-medium)", EFM participants (customer contract partners (retailers)) will hand over data protection notifications to the end-customers relating to issuing the customer medium.</p>
<p>2. Right of objection</p> <p>The Association of German Transport Companies should make an agreement with their customer contract partners (retailers) that when concluding the agreement the customer states in writing whether or not he wishes to object to his personal data being transferred or used for advertising and / or marketing research and opinion research. It must be ensured that authorised third parties also adhere to these restrictions.</p>	<p>The "Participation contract" (participation agreement between the VDV-Kernapplikations GmbH & Co. KG as application issuer and transport companies acting as customer contract partners (retailers) in the EFM system - a draft agreement is available) shall include an obligation for companies who take on the role of a customer distribution partner.</p>
<p>3. Options</p> <p>Based on the information with regard to contractually related data processing, passengers must be able to decide freely between anonymous travel and specific service offers (for</p>	<p>The passenger can choose between anonymous / pseudonym (also against cash payment) and a personalised electronic ticket (e.g. season ticket, student/scholar</p>

<p>example best pricing).</p>	<p>tickets).</p> <p>Core Application envisages the following services for the purchase of tickets for public transfer or rather to make use of public transport:</p> <ul style="list-style-type: none"> * Authorisations regarding the stored value units on the user-medium (with a shadow account at the customer operating partner) * Authorisations with pseudonym settlement following pre-payment onto a customer account and direct debit of the service against the payment received in advance. * Authorisation by payment through direct debit authorisation (eTicket card bound to a bank account)
<p>4. Data economy</p> <p>All service characteristics and business processes are to be designed according to the principle of data avoidance and data economisation (Section 3a BDSG). Creating customer-related motion profiles must in particular be avoided. This means:</p> <ul style="list-style-type: none"> * Data for planning purposes and for the optimisation of the offer must be raised anonymously or must be made anonymous. * As far as data is required for specific service offers or complaints management, such data must be raised via pseudonym and stored in a way that any connection to the affected passenger is impossible without his knowledge and will. * In the event that user-related data is recorded on mobile storage mediums (chip cards) for the purpose of complaints management, the passenger 	<p>As a rule, collecting data in the systems for settlement and planning purposes and for the optimisation of travel offers only takes place without assigning such data to a specific person - only data required for this purpose is linked.</p> <p>When using data derived from the use of public transport, "aliases" are stored and only assigned to a single person for settlement purposes (the account holder).</p> <p>Use-related data in the user-medium are overwritten at the next use (max. 10 transactions are stored in the medium, in particular so that the customer can read out the last uses, if he wishes to do so).</p> <p>These transactions are also transferred to the background system which is responsible for the relevant travel entitlement.</p> <p>The KA NM- SPEC specifies contents which serve as statistical evaluations (as a substitute for expensive traffic</p>

<p>must be given the possibility of deleting this data at his own risk.</p>	<p>surveys) or which are necessary as an element in the security concept.</p>
<p>5. Separate processing</p> <p>The relevant required technical and organisational measures must always be taken to ensure that the information raised can be processed separately for different purposes (No. 8 of the attachment to Section 9 BDSG).</p>	<p>In a participation contract, VDV-KA-KG obligates the customer contract partners (retailers) to store customer master data or invoice data in separate systems so that no customer-related travel profile can be established.</p> <p>Data is only linked for billing purposes.</p> <p>Employees of the customer contract partners (retailers) processing the personal data are obliged to protect such data and comply with telephone secrecy in terms of BDSG and LDSG [Landesdatenschutzgesetz = State Data Protection Act].</p>
<p>6. Restrictions on the use of ticket data</p> <p>In addition, no customer or card related evaluations are allowed for third-party purposes. For invoicing purposes within the linked transport system only pseudonym card-related data may be transferred.</p>	<p>The specification envisages that only card-related (that is to say "authorisation" related) data may be communicated between the EFM system operators.</p> <p>Customer-related data may only be drawn up with the customer's written approval and by his own customer contract partner (retailer).</p> <p>In the "application to issue an eTicket (user-medium)" the customer is advised of the type of data processing even if this contract is not mandatorily drawn up in the event of acquiring an anonymous authorisation.</p>
<p>7. Prior check</p> <p>Prior to commissioning the EFM, the company data protection officers shall conduct a prior check (Section 4 of Para 5 and 6 BDSG) and document it.</p>	<p>This shall also be guaranteed by the EFM systems operator. This obligation must be included in the Core Application participation contract for those companies</p>

	participating in the VDV-KA.
<p>8. Access authorisation</p> <p>Read access for control personnel must be restricted to the data required for control, in particular in connection with the passenger's storage medium.</p>	<p>Only area and time-related authorisations are controlled.</p> <p>Where the application is personalised, the customer's profile is secured by means of cryptography.</p> <p>Access to the customer's profile is only possible via an asymmetric authentication between the terminal and the user-medium or if the customer enters a PIN.</p> <p>Personalised authorisations are only implemented in exceptional cases by entering data into a customer profile. In most cases, personal data is only stored in a background system.</p> <p>User-related data is only seen by the control personnel during the ticket control process and is not collected electronically for further processing.</p> <p>Personal data (name, gender, date of birth) are stored in terms of authorisation in the event that such personal data has to be controlled (e.g. scholars, students).</p>
<p>9. Design of the system components in a manner compatible with data protection</p> <p>The system's components, which are operated by the passengers, must be designed in such a way that they fulfil data protection compatibility:</p> <ul style="list-style-type: none"> * by not providing any possibility for unauthorised persons at terminals for cashless payment to become aware of data entered, in particular authentication data, * by not publicly discriminating the affected persons in the event of error messages 	<p>Automatic controls and data capturing by terminals are only carried out with anonymous authorisation data. All transactions are only carried out following authentication.</p> <p>Customer data at self-service sales terminals / in the Internet are only shown after a PIN is entered (VDV KA-KUSCH Spec).</p> <p>Telephone services are only carried out following password authentication.</p>

<p>signalised by access capturing systems,</p> <p>* by allowing the passengers to read the content of the chip card at any time and to a reasonable extent.</p>	<p>Error messages in connection with the presentation of the user-medium on devices with a customer interface will not include the reason for the error.</p>
<p>10. Protection against abuse</p> <p>Precautions (for example blocking, encryption) must be taken which reasonably protect the passenger against improper use of the data by a third party in the event of a loss of the storage medium.</p>	<p>The customer can block the application and individual authorisations.</p> <p>For performance reasons there is no encryption when accessing the application directory and authorisations.</p> <p>Authorisations are stored with coded data components and transferred to various EFM systems for processing purposes. ORG-IDs, which are assigned by VDV-KA KG, are confidential. Number codes for places / stops / railway stations are not published.</p> <p>Write processes and transactions are generally only carried out following cryptographic authentication and secured by a signature.</p>
<p>11. Deletion</p> <p>The business process for storing personal data must be as short as possible. Standard periods for the deletion of data for the various business processes must be defined (Section 4e Sentence 1 No. 7 BDSG). Data stored in the terminals must be deleted following the successful data transfer to the customer contract partner's computer.</p>	<p>The deletion of data must be guaranteed by the EFM system operators by way of a participation agreement.</p> <p>The time limits are defined subject to the business processes and coordinated with the responsible data protection officer.</p>

The requirements directed at the so-called customer contract partners (retailers) (but also in part at the EFM system operators) can already be derived from the standards drawn up by the work group of the data protection authorities and the explanations with regard to their implementation.

1. To ensure transparency for the customers, the customer contract partners (retailers) provide users with a document containing information describing the data processing operations and the data which is stored on the user-medium in a manner that the customer can understand. As far as the customer medium is a chip card which corresponds to the stipulations of Section 3 Para 10 BDSG, this information paper must also include all information which is listed in Section 6c Para 1 BDSG.

Furthermore, the measures required to comply with Section 6c Paras. 2 and 3 BDSG must then also be taken. This applies in particular to Para 2 (provision of readers for the implementation of the right of information), as Para 3 should have now been fulfilled per se.

2. On concluding the customer contract ("application to issue an eTicket card (user-medium)"), the customer contract partners (retailers) are obliged to provide customers with the possibility of giving a written statement as to whether or not they agree to their personal data being transferred or used for advertising and / or marketing research and opinion research. They shall ensure that even authorised third parties comply with such restriction.
3. The customer contract partner (retailer) must inform the customers as to the existing possibilities for an anonymous payment and use of the transport systems.
4. To fulfil the requirement of data avoidance and data economisation (Section 3a BDSG), customers' master data and relevant data otherwise raised for accounting purposes for the journey are processed separately for non-anonymous use. Data which serves as the basis for statistics, planning and the optimisation of travel offers is stored and processed without any reference to the person. The customer master data and invoice data are only linked for accounting or complaints handling purposes.
5. Only data in pseudonym form (data related to the authorisation) may be exchanged for accounting purposes between the EFM systems operators. In the event of a non-anonymous use, only the customer contract partner (retailer) with whom the customer has concluded the customer contract may access customer identity information with the customer's written approval.
An authorised terminal can only access personal data stored on the user-medium after a PIN has been entered or following asymmetric authentication.
6. As far as there is no prescribed legal retention period for personal data or pseudonym accounting data, all personal or pseudonym data which arose during a journey must be completely deleted or anonymized by the EFM operator respectively the customer contract partner (retailer).
7. EFM operators and customer contract partners (retailers) must ensure that
 - when using the terminal for cashless payment, unauthorised persons are prevented from becoming aware of the data entered in particular authentication data,

- error messages are not signalled to the access capturing systems in a way which could publicly discriminate against the affected persons,
 - error messages to the customer interface cannot disclose the reason for the error,
 - passengers are given reasonable opportunity to read the content of the chip card at any time (Section 6c Abs. 2 BDSG).
8. Within the framework of a prior check, the company data protection officers of the EFM operating companies and the customer contract partners (transport companies) will examine whether the requirements described in 1 - 7 are fulfilled and whether, according to the VDV Core Application, the technical and organisational measures have been implemented to protect customer relationship communication against unauthorised data access (e.g. access by control personnel, loss).

The prior check must be documented for audit purposes (e.g. by the competent data protection control authorities).

Modifications

Draft 1	Main authors : Gilles de Chantérac Michel Arnaud Jean-Louis Graindorge	Jan2009- feb 2009 Version 1.4 sent to the consortium on Feb. 24 th
Preliminary version 1		Discussed in a French Workshop 10/03/09
Draft 2		Version 2.2 sent for comments to the consortium 18/03/2009 Version 2.3 sent to the commission for information 23/03/2009 Version 2.4 becomes preliminary version 2
Preliminary version 2		Presented at the IFM Forum (Delft, 30/03/09)
Draft 3		Version 3.1 sent for comments to the consortium 22/06/09
Draft 4	Michel Arnaud and other contributors	Version 4.3 to be sent for comments to the consortium and contributors in December 10, 2009