Functional survey of existing sets of privacy protection rules applicable to transport IFM applications by national institutions and regulations in different contractors European countries.

Deliverable 2.1

March 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**

This report constitutes deliverable D2.1 of the IFM project.

The survey was sent namely to 15 members of the IFM consortium and was available on the project website since July 2008.
Although reminders were sent, transport authorities and operators representatives appeared to be reluctant to participate:

- The format of the questionnaire, based upon the model of ISO 24014-1 standard, made it difficult for representatives to translate it into practical terms in their own environment.
- The fact that one of the most frequently used memory cards had just been hacked made the subject very touchy to some organisations that were facing communication crisis.
- The difficulty to step from theoretical objectives to practical rules also appeared clearly.

All these elements have inspired a new approach for phase 2 of this work package in order to initiate a privacy model to be proposed as a final objective for Interoperable fare management in Europe. A working paper on this issue is proposed at Steering Committee meeting in Cologne on March 13, 2009.

For further information please contact

Work package WP2

University of Paris X

Prof. Michel Arnaud
Phone ++33.685734057
E-mail: michel.arnaud@u-paris10.fr

Main authors

Michel Arnaud
Jean-Louis Graindorge
Gilles de Chanterac

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**

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

Table of contents

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

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

0 List of abbreviations

IFM	Interoperable Fare Management
ITSO	Integrated Transport Smartcard Organisation; UK Standard for nationwide Interoperable Electronic Fare Management
RATP	Régie Française des Transports Parisiens
SNCF	Société Nationale des Chemins de Fers Français
TA	Transport Authority
TO	Transport operator
TTP	Trusted Third Party
VDV-KA	VDV Core Application, German Standard for nationwide Interoperable Electronic Fare Management

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

1 Introduction

As new payment facilities bring new services to customers, transport operators break a traditional protection of privacy which prevailed in the past with 'mass transit'. When a customer subscribes for tariffs, loyalties or special means of payment, he willingly delivers appropriate private data that are necessary to open his rights to these facilities and to allow their operation.

The validation process also allows recording of his trips, necessary for fraud protection programs, and sometimes for the payment itself. Anonymously, these data are useful to monitor capacities and schedules, tariffs, etc… Once they exist, transport operators and authorities also wish to use them for individual marketing purposes.

Each stage of progress towards seamless travel brings the customer new risks that his privacy is attacked: personal data can be captured from the fare device by different front-end equipments. They can also be exchanged between back-offices. Therefore, new functional facilities allowed by multi-application fare devices generate a new risk for privacy: Personal data a customer has accepted to communicate to one of his service providers *-e.g. his bank or his domestic IFM manager-* could be captured from the fare device by another one *-e.g. a foreign IFM manager-* .

This survey investigates and compares National and European privacy protection regulations applied to public transports as well as existing sets of privacy protection rules implemented in IFM applications by transport agencies and operators. To which extent privacy protection rules are applied and how they are perceived and dealt with is also an important aspect in order to measure the degree of awareness and responsibility on privacy issues shared by transport operators and agencies.

A summary of privacy protection regulations in the following core countries: France, Germany, United Kingdom, is proposed as well as the results of the WP2.1 survey on privacy protection functions in organisational models for some European fare management systems in the same three core countries. Since representatives of France, Germany and UK are involved in the IFM project, questionnaire results can be corroborated. Sweden has finally sent on March 3, 2009 answers to a simplified questionnaire. IFM systems in the Netherlands and Portugal should be added for this survey so that a relatively large area of Europe could be taken into account if appropriate answers to the questionnaire are provided, which is not the case up to now. Topics covered by the IFM project questionnaire tend to define various organisations role within IFM network, their needs in terms of personal data, how they implement traveller's privacy protection, which solutions are sought.

The present documents couldn't consider the migration steps as they were defined by WP3 after the workshop held on the 18th of December, long after the questionnaire was launched.

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

The privacy risks will largely differ according to the interoperability context of each step towards the vision that this workshop described.

1. **Co-existence of existing transit application into the same media :No impact on privacy requirement**
   In this context, customers go on using locally transit applications already in place. No change is then required in back office system in term of privacy data management and there is no personal data transfer needed between IFM schemes.
   The potential risk, that a third party may read information of another party when presenting a multi application, is not new. With dedicated single application customer media, anyone is already able to read silently data via device contactless interface.
2. **Introduction of a common EU status application: New impact but …**
   The EU Status application is a new application to be defined. Privacy rules to be applied for such application can be different and likely stricter than existing ones as applicable privacy requirements shall take into account rules from all EU domestic privacy data protection authorities.
3. **Introduction of a common IFM application: Same as above …**
   Same requirement as in 2. for the EU status application will apply.

These differences will be re-introduced in ulterior work phases of WP2.

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

2 Definitions of privacy related terms

Definitions need to be given in the first place in order to specify characteristics of personal data, of actors involved in their processing and of types of regulations to be applied in the IFM architecture.

2.1 Personal data

Any information concerning an identified or identifiable natural person is deemed to be personal data[1].

2.2 Special personal data

Special personal data are all personal data that provide information on a person's characteristics apart from identity data (name, birth date and place, address, id card number, etc..) :

- religious or philosophical beliefs,
- race,
- political opinions,
- health,
- sex life,
- membership of a trade union,
- personal data connected with a person's criminal behaviour,
- personal data connected with unlawful or objectionable conduct for which a ban has been imposed (a street ban, for example).

Different types (related to privacy issues) of personal data are used in Transport applications:

- Identity - name, age, address …
- Transport Profile - student, worker, usual trips …
- Other profiles - payment means …
- Tickets purchased and validated - time, localisation …

2.3 Data subject

The person to whom the personal data relate.

2.4 File

Any structured set of personal data, irrespective of whether this data set is centralised or dispersed along functional or geographical lines, that is accessible according to specific criteria and relates to different persons.

2.5 Personal data processing

Any operation or any set of operations upon personal data, such as:

- collecting, recording, organisation, storage,
- adaptation or alteration, retrieval,
- consultation, use,
- disclosure by transmission, dissemination or otherwise making available,

[1] ARTICLE 29 WORKING PARTY opinion 4/07 on the concept of personal data : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

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

- alignment or combination,
- blocking, erasure or destruction.

2.6 Controller

Natural person, legal person, administrative body or any other entity, which, alone or jointly with others, determines the purpose of and the means for processing personal data.

2.7 Processor

Person [Natural person, legal person, administrative body or any other entity] which processes personal data on behalf of the controller without coming under the direct authority of that party.

2.8 Third party

Any party, other than the data subject, the controller, the processor or any person under the direct authority of the controller or the processor, who is authorised to process personal data.

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

3 Privacy regulation main aspects

3.1 International legal basis

3.1.1 OECD

The recommandation of the OECD Council concerning Guidelines governing the protection of privacy and transbirder flows of personal data was adopted in September 1980. It affirms, that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information; that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices; that transborder flows of personal data contribute to economic and social development; that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows. The document give a first set of definitions of main terms.

3.1.2 Council of Europe

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (convention 108) was adopted by the Council of Europe in January 1981 and entered in application on 1st October 2005. This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.

3.1.3 European Directives

A) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;

Although based on the same basic principles laid down in a Council of Europe Convention, these laws differed considerably in detail. Because this was considered to influence competition and thus the well functioning of EU's internal market, pressure increased for a more harmonised environment. Developments in the ICT-field added to the need for a common set of data protection rules, specifying the Council of Europe Convention.

Directive 95/46 is the central piece of legislation on the protection of personal data in Europe. The Directive stipulates general rules on the lawfulness of personal data processing and rights of the people whose data are processed ('data subjects'). The Directive also provides that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation.

A Directive on privacy and electronic communications was adopted two years later.

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

B) Directive 2002/58 concerning the procedding of personal data and the protection of privacy in the electronic communications sector

It updated and replaced the former Directive on privacy and electronic communications. It regulates areas which were not sufficiently covered by Directive 95/46

C) *Main principles*

Member States had to implement the directive into their national legislation2. National data protection Commissioners have been appointed in all of them3.

Persons whose data are collected have a number of rights among others the right of access, rectification, erasure, blocking and objection.

- Transparency principle

Everyone must be informed about what is done with his/her personal data.
The data subject has the right to be informed when his personal data are being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. (art. 10 and 11)

Data may be processed only under the following circumstances (art. 7):

- when the data subject has given his consent
- when the processing is necessary for the performance of or the entering into a contract;
- when processing is necessary for compliance with a legal obligation
- when processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12)

[2] communication from the Commission to the European Parliament and the Council o the follow-up of the work programme for better implementation of the data protection directive:
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[3] http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm

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

- Legitimate purpose

Personal data are only collected for a specified predetermined purpose. These can be processed for that purpose and under certain conditions for other purposes.

- Proportionality principle

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (art. 6)

The data subject may object at any time to the processing of personal data for the purpose of direct marketing. (art. 14)

- Exonerations

If you are able to exercise any actual power or influence, whether or not by means of a computer system, over the data, you have to comply with the regulations. If you cannot exercise power or influence over the personal data, you do not have to comply with the regulations. A number of forms of processing are explicitly exempted from the regulations.

The regulations do not apply if you process personal data solely for personal or home use.
This may be the case with personal work notes, or a tray with business cards of persons who are regularly contacted, which an employee of a company keeps as a reminder for himself. It does not matter in these cases that the employee's secretary may become acquainted with these data in special circumstances.

The regulations do not apply if your data processing falls under one of the designated exempted forms of processing.
These exempted forms of data processing are:

- processing by or on behalf of intelligence or security services;
- processing for purposes of implementing police tasks;
- processing by municipalities in the municipal personal records database;
- processing for purposes of implementing a judicial act and certificates of good behaviour.

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

3.2 Recommendations and Interpretation of current laws

3.2.1 International: APEC privacy framework

The Asia Pacific Economic cooperation (APEC) privacy framework is mentioned as a reference in the international standards; thus it could be useful to mention it. It publishes a set of recommendations that Member Countries should apply as far as possible.

3.2.2 Europe: Article 29 Data Protection Working Party

This European body has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC[4].

The Article 29 WP was set up to achieve several primary objectives:

- To provide expert opinion from Member State level to the Commission on questions of data protection.
- To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities.
- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
- To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

3.3 Standardisation issues: ISO

3.3.1 ISO reference standards

- ISO 24100 Intelligent transport systems, Wide area communications, Basic principles for personal data protection in probe vehicle information services ".
- ISO/IEC 17799 Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC 18028 Information technology -- Security techniques -- IT network security

[4] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

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

- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems

Hereafter we mention some elements that have been extracted of a so-called Liaison Organisation Contribution from ISO/IEC JTC1/SC17 N 3641. It is a very recent document (04/02/2009). The requirement for this report was originated from discussions with ISO TC204 concerning the use of personal data in Intelligent Transport Systems.

"The pressures for business case justification initially sustains such developments without a clear legal position, and it is necessary not only to consider the technical and engineering possibilities, but to ensure that they evolve within a framework of generally (internationally) accepted data protection principles, and of course within National data protection legislation."

The interest of the document is that it makes a deep analysis of the existing text to formulate its own recommendations.

A) Recommendations

Avoidance of harm
Shall recognize the interests of the individual to legitimate expectations of privacy, personal information protection and should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations shall take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
(APEC Privacy Framework Part iii)

B) Fairly and lawfully
All personal data shall be obtained and processed fairly and lawfully;
(APEC Privacy Framework Part iii, I,; EU Privacy Directive C3 Article 5; OECD Part 2, 7)

C) Specified, explicit and legitimate purposes
All personal data shall be collected for specified, explicit and legitimate purposes
(APEC Privacy Framework Part ii (CI.13); Part iii (CI. 1)

D) Explicit and legitimate and must be determined at the time of collection of the data

The purposes for which personal data are collected shall be determined at the time of the collection of the data and shall be explicit and legitimate at the time of collection of the data and use of the data limited tothe fulfilment of those purposes (or such others as are not incompatible with those purposes specified); andthe subsequent use shall be limited to the fulfilment of those purposes (or such others as are notincompatible with those purposes). All personal data collected shall be adequate, relevant and notexcessive in relation to the purposes for which they are processed;
(EU Privacy Framework. 7.14.11 Cl 28, 56, 57; 7.19.5 (c) ; OECD Part 2. Cl.9)

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

E) Not further processed in a way incompatible with the purposes for which it was originally collected

All personal data shall not be further processed or used in a way incompatible with the purposes for which itwas originally collected.
(EU Privacy Directive 7.14.1.1 Cl. 28,29; 7.19.5 (b); 7.40.1 (2); OECD Part 1 Cl 9, 24)

F) Not be disclosed without the consent of the data subject

Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Clause 4.4 except: (a); or (b).
a) where the data subject has freely and unambiguously given his/her consent
b) by the authority of law of the Country
c) processing is necessary for the performance of a contract to which the data subject is party or in order to
take *steps at the request of the data subject* prior to entering into a contract; or
d) processing is necessary for compliance with a legal obligation to which the controller is subject; or
e) processing is necessary in order to protect the vital interests of the data subject; or
f) processing is necessary for the performance of a task carried out in the public interest or in the exercise
of official authority vested in the controller or in a third party to whom the data are disclosed; or
g) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the
third party or parties to whom the data are disclosed, *except where such interests are overridden* by the
interests for fundamental rights and freedoms of the data subject defined above.
(EU Privacy Framework. Cl 28, Cl 30 & Section D11, Cl7.19.13 2(d); OECD Part 1. Cl.10; OECD Part 2.
Cl.9; APEC Privacy Framework, Part iv Cl.29)

G) Adequate, relevant and not excessive in relation to the purposes for which they are collected

All personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
(EU Privacy Framework. Cl 28, Cl 30 & Section D11, Cl7.19.13 2(d); OECD Part 1. Cl.10; OECD Part 2.
Cl.9; APEC Privacy Framework, Part iv Cl.29)

H) Accurate and, where necessary, kept up to date

All personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they
were collected or for which they are further processed, are erased or rectified.
(APEC Privacy Framework v1 Cl.21; EU Privacy Directive, Section 1. 7.19.5; OECD Part 1, Cl 8)

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

I) Identification of data subjects for no longer than is necessary for the purposes for which the data were collected

All personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

(APEC Privacy Framework ; EU Privacy Directive; OECD)

J) Restricted to those who have a demonstrable 'need to know'

Access to personal data shall be restricted to the minimum number of persons who have a demonstrable 'need to know'.

EXAMPLE in a situation where a law of the land has been allegedly infringed, an enforcement officer should have access only to information necessary to enforce, and not all information pertaining to the subject individual, his ownership of vehicles or other personal data. That information may for example only identify a vehicle and this data may be passed to a prosecution system. A national prosecution service, shall of course have need of access to much information concerning the accused person in order to effect a prosecution, but all of this information should not be available to all enforcement officers, and should not be made available without a justifiable need to know.

(OECD Para 1, 59)

K) Clear and accessible

Personal information controllers shall provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

a) the fact that personal information is being collected;

b) the purposes for which personal information is being collected

c) the types of persons or organizations to whom personal information might be disclosed

d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information.

(APEC Privacy Framework Part iii, Cl.15,20 ; EU Privacy Directive 7.9.1.2;)

L) Security safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

(APEC Privacy Framework Part iii, Vii Cl.22 ; OECD Part 2. Cl.11)

M) Cumulative interpretation of multiple recommendations

In the development of USSN systems and standards, we are advised by legislators and lawyers that the recommendations cannot just be taken individually in isolation, but the combination of the recommendations may infer interpretations, this has significant implications. Lawyers often refer to this as 'cumulative

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

4 Legal framework for privacy in public transport

Specific data privacy protection legislation is generally achieved by National legislation, and for a variety of social, cultural, economic and legal backgrounds, vary from country to country. However, the general principles are common, and due to provisions made by trading blocks such as the European Union, and APEC, in many cases, while there may be specific National aspects to data privacy and data protection, there are common aspects that are global. Common guidelines are provided by regulations such as the Data Protection Directive of the European Union, the APEC Privacy Framework and OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data.

4.1 European legal framework for privacy in public transport

Article 29 Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC[5].

A specific group on e-ticketing in public transport has been set up within ARTICLE 29 Working Party and extracts from Working Paper about e-Ticketing in Public Transport adopted by the ARTICLE 29 working party at the 42nd meeting, 4-5 September 2007, Berlin are presented below.

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.

4.1.1 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

[5] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

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

personal data; generally speaking, they should reconcile the right to free movement of individuals with the requirements of effective public transportation.

4.1.2 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:

4.1.3 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*

A PTA 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*

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

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.

4.2 Public transport privacy regulations in Member States

4.2.1 France

In France, the CNIL (National Commission for Informatics and Freedom) controls personal data protection processes mainly in public data bases and for a lesser extent in privately owned data bases. For e-ticketing in public transport, the CNIL has completed an extensive consultation with transport operators and agencies before issuing, in July 2008, a general authorisation framework that they must respect to set up their electronic ticketing systems. The transport operators and authorities that are engaged to comply with the rules that are defined in the general framework are no more subjected to a specific authorization and shall only declare their systems once.

As it is possible to trace any passenger using a transport e-card, which is in contradiction with the fundamental and constitutional right to be able to travel freely as well as privately, respect of these basic principles implies that the option to travel anonymously has to be offered permanently. Types of personal data are strictly defined according to their corresponding uses (e-ticketing sale and validation, statistical analysis, quality check and fraud detection). Transport operator and agency employees access to traveller's personal data is strictly controlled to prevent any misuse of personal data stored on computer disks. All collected data are stored during the length of contract validity (monthly, bi-yearly, yearly), two years are added for commercial use (contacts with customers and prospects). As personal data are entered in the system, validation data (which means identification data: last name, first name, subscription number of the traveller) are anonymised immediately. This anonymisation is done either by suppressing card number in the data base or by using a cryptographic algorithm to mask the card number (strong hash code).
Persons likely to be registered in the payment incident file must be informed when the contract is subscribed, before their coordinates are added to the file and the transport title is cancelled. Information related to payment incidents are immediately cancelled from the opposition list as soon as payments are made. If not paid, they will be kept for a maximum of three years. Access and rectification rights are to be guaranteed according to chapter V of the 6th of January 1978 modified law by the services to which the person in charge has assigned this task.

4.2.2 Germany

In Germany, the Federal Commissioner for Data Protection and Freedom of Information has counterparts in each 'federal sate' dealing with privacy issues in the administration and municipalities. There is a supervisory authority of the so-called non-public sector (Düsseldorfer Kreis)in cases where private economic

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

entities (enterprises, associations and self-employed) apart from telecommunications and postal services are involved. The Conference of Data Protection Officer of the Federation and the federal states is the body that deals with current issues of data protection in the public sector in Germany and an opinion on them. The conference consists of the Federal Data Protection Commissioner and the country's Data Protection Officer of the 16 federal states.
Information requests and complaints in the sphere of radio stations under public law may be referred to the respective data protection officer. However, in the 'federal states Berlin, Brandenburg, Bremen and Hesse, the data protection commissioner is also competent for the administrative body of such radio stations under public law. Specific regulations coordinated between the KA appliers, the VDV-Kernapplikations GmbH & Co.KG and DPOs are negotiate based on the "Framework Directive Electronic fare management (EFM) - Privacy basic requirements" for e-ticketing in public transport and regulations will be issued in 2009.

4.2.3 United Kingdom

In the United Kingdom, the Information Commissioner's Office supervises offices in Scotland, Wales and Northern Ireland. The ICO has issued a technical guidance note to explain and illustrate the ICO's view of what is personal data for the purposes of the Data Protection Act 1998. It applies only to information which falls within the definition of 'personal data' and relates to an identified or identifiable individual. When considering identifiability it should be assumed that someone is not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals.
The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

To our knowledge there is no specific regulations issued for e-ticketing by ICO.

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

5 Privacy within IFM

These aspects on general data privacy and protection should be incorporated into the architecture and design of all e-ticketing standards, systems and implementations. Within the IFM project and according to ISO 24014-1:2007 - Public transport - Interoperable fare management system - Part 1: Architecture, there is a need to coordinate action to define a joint strategy for media, back-office architecture, security and privacy models. If fares can be anonymous (e.g. single ticket) or restricted to one customer (e.g. social fares, season tickets), personalised cards allow personalised services for traffic information, payment methods (e.g. orders on accounts, stored value) and special offers (e.g. special student offers). For transport operators and agencies, there is a need to share traveller's personal data to pool common invoicing processes and to secure systems against fraud.

However, ISO 24014-1:2007 - Public transport - Interoperable fare management system - Part 1: Architecture stresses on the importance of the following aspects in 9.1 Protections of the interests of the public: - Privacy. Information generated by the IFMS shall be protected as required by applicable laws. These principles are of general nature and are not further specified in this standard, but should nevertheless be accounted for and followed within any Organisation responsible for public transport services.

As for privacy international and European regulations impose restrictions on the collection, storage, processing and dissemination of data relating to individuals and their behaviour. Some countries require a fully anonymous system. For that reason, the IFMS has to safeguard users' privacy. To achieve this, at least the following rules must apply:
- Only relevant personal data needed for the operation of the IFMS is requested from the Customer.
- The itemised disclosure of service consumption on an invoice is an option that can be chosen by the Customer.
- A IFM Actor cannot disclose Customer related information to third parties without specific authorisation from the Customer.
- Within the IFMS the Customer specific data is only handled in connection with the identification number of the Contract (implicit or explicit) between the Customer and Product Owner. A link between the Contract number and the name of Customer can only be achieved by the contractual partner at the request of the Customer.

5.1 IMF architecture and privacy concerns

The common IFM System Architecture described in the standard ISO EN 24014-1 (shown in Figure 1) describes the central functions like IFM Manager, Security Manager and Registrar.

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

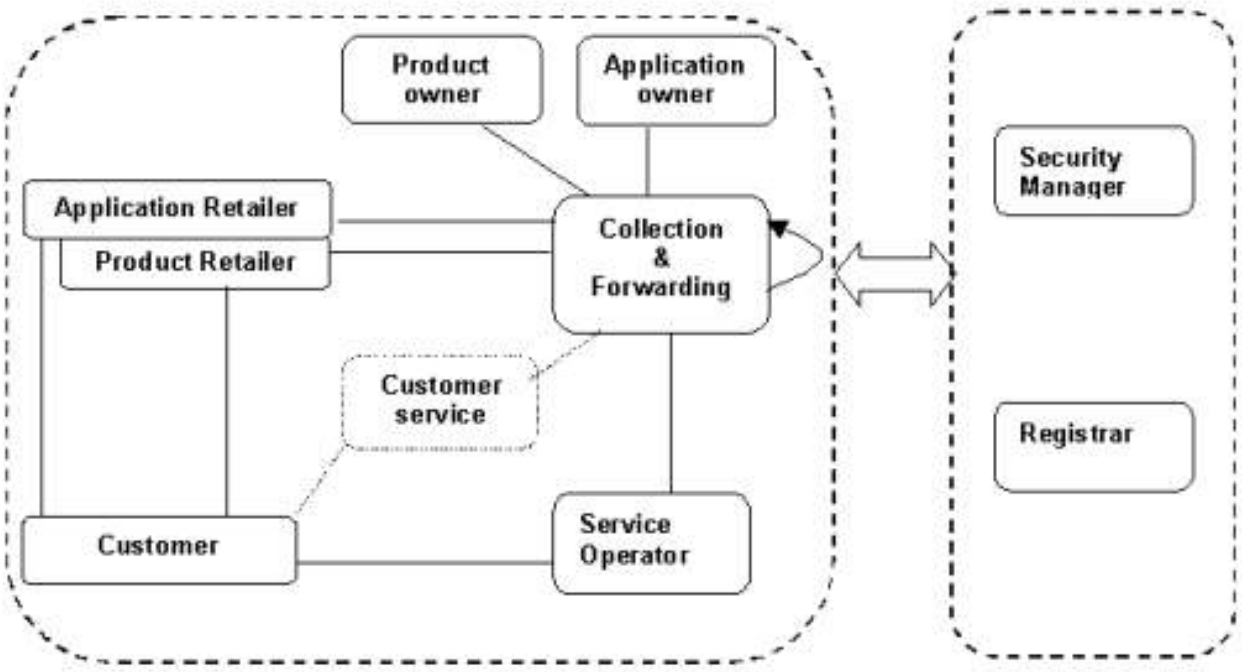

Figure 1 — The two IFM domains (operational and management Entities)[6]

The following types of actors are defined in ISO 20214:

Customer	Holds an Application. Acquires Products in order to use the public transport services.
Service Operator	The service operator provides service to the customer against the use of a Product.
Application Owner	Holds the Application Contract for the use of the Application with the customer.
Application Retailer	Sells and terminates Applications, collects and refunds value to a customer as authorised by an Application owner. The Application Retailer is the only financial interface between the customer and the IFMS related to Applications.

[6] Source: ISO/EN 24014-1:2005

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

Product Owner Is responsible for his Products.

Functions of Ownership:

Specifying pricing, Usage Rules and Commercial Rules.

Functions of Clearing:

Trip reconstruction - Product aggregation based on received usage data using Product definition rules

Linking of aggregated usage data with acquisition data

Preparation of apportionment data based on Product Specification

Functions of Reporting:

Detailed:

- acquisition data with no link to usage data within the reporting period
- usage data with no link to acquisition data within the reporting period
- linked aggregated Product data within the reporting period

Summary:

- apportionment data and clearing report

Total acquisition data

Product Retailer Sells and terminates Products, collects and refunds value to a customer as authorised by a Product Owner.

The Product Retailer is the only financial interface between the customer and the IFMS related to Products.

Security Manager The Security Manager is responsible for establishing and the coordination of the Security Policy and:

- certification of Organisations, Application Templates, Components and Product Templates
- auditing of Organisations, Application Templates/Applications, Components and Product Templates/Products
- monitoring the system
- operation of the security of the IFMS, e.g. key management.

Registrar After the certification, he [the Registrar] issues unique registration codes for Organisations, Components, Application Template, Product Templates. The Registrar function also issues unique identifiers or rules for generating unique identifiers for the Applications, Products and messages.

IFM Services are defined as the following :

Customer service Subject to commercial agreements may provide “helpline” and any similar facilities including stolen and damaged Customer Medium replacement and consequential Product reinstalling.

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

Collection & Forwarding

The role of Collection & Forwarding is the facilitation of data interchanges of the IFMS. The general functions are data collection and forwarding. They contain at least the following functions:

Functions of Collection:

Receiving Application Template from Application Owner

Receiving Product Template from Product Owner

Receiving data from Service Operators

Receiving data from Product Retailer

Receiving data from Application Retailer

Receiving data from other Collection & Forwarding

Receiving security list data from Security Manager

Receiving clearing reports from Product Owner

Consistency and completeness check of the data collected on a technical level

Receiving address list of all Entities in the IFM from the Registrar

Functions of Forwarding (see note below):

Forwarding “Not On Us” data to other Collection & Forwarding.

Recording “Not On Us” data

Forwarding data with corrupt destination address to security manager

Forwarding “On Us” data to the Product Owner for clearing and reporting

Forwarding clearing reports, Application Template and Product Template, security list data to the Product Retailer and Service Operator

Forwarding Application Templates, security list data to the Application Retailer and Service Operator

NOTE: “ON US and NOT ON US” concept:

- A specific Collection & Forwarding function is to collect data from one IFM Entity and forward it to other IFM Entities.
- Logically there may be several COLLECTION & FORWARDING Entities within the IFM.
- IFM Entities may be linked to different COLLECTION & FORWARDING but each Entitiy can only be linked to one.
- The concept of "ON US and NOT ON US" addresses this connectivity functionality. Data held by a specific COLLECTION & FORWARDING is either "ON US" or "NOT ON US" data
- Data collected by a specific COLLECTION & FORWARDING addressed to IFM Entities directly linked to this COLLECTION & FORWARDING is termed "ON US" data.
- Data collected by a specific COLLECTION & FORWARDING addressed to IFM Entities not linked to this COLLECTION & FORWARDING is termed "NOT ON US" data.

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

Four steps have to be validated according to privacy regulations:

1) Personal data are entered in the Product Owner data base controlled by security manager (only relevant personal data needed for the operation of the IFMS is requested from the Customer).
2) Data related to the identification number of the Contract (implicit or explicit) between the Customer and Product Owner are put on the media. (A link between the Contract number and the name of Customer can only be achieved by the contractual partner at the request of the Customer.)
3) Transport transaction data are put on the media (usually they are anonymized)
4) Reporting activities are performed in order to split payments between service operators and products owners and fight fraud.

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

6 Results of IFM project questionnaires

A questionnaire has been sent out to IFM partners, based on IFM concepts and architecture. Topics covered by the IFM project questionnaire tend to define various organisations role within IFM network, their needs in terms of personal data, how they implement traveller's privacy protection, which solutions are sought.
Although few answers have been collected, results can be drawn from the very fact of scarcity of answers which tends to prove that an important gap exists between IFM conceptual framework and real life transport applications. The definition of personal data can pose problems since each transport operator or/and agency has its own approach for processing them.

6.1 Results presentation

6.1.1 Your organisation role

- **Number of stakeholders in IFM organisation**

ITSO (UK)
ITSO Card
Media: 11
Application : 11
Product : 11

RATP (France)
Navigo
Media owners 1
Media retailers 4
Application owners 1
Application retailers 4
Product owners 1
Product retailers 4

VDV (Germany)
eTicket Deutschland
Media owner about 14 this time
Application owner 1
Application retailers about 14 this time
Product owner about 14 this time
Product Retailers about 120
Service operators about 120

- **Roles your organisation plays**

ITSO (UK)
ITSO card
Collection & Forwarding
Security
Service providers

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

Customer service providers

RATP (France)
Navigo
Media retailer
Application retailer
Product retailer
Collection & Forwarding
Security
Service provider
Customer service provider

SNCF (France)
TER
Media owner and retailer
Application owner and retailer
Product owner and retailer
Service provider
Customer service provider

VDV (Germany)
eTicket Deutschland
Media owner
Application owner (is also responsible for security management, certification and registration)
Product owner
Service provider
Customer service provider

- **Referring to European working party definitions, roles your organisation fulfils**

ITSO (UK)
ITSO card
Controller
Processor

RATP (France)
Navigo
Controller
Processor

SNCF (France)
TER
Controller
Processor

VDV (Germany)
eTicket Deutschland

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

Controller
Processor

6.1.2 Your organisation needs

- **Reasons for accessing data about identity, transport and payment**

RATP (France)
Navigo
To answer customer's demand
To improve customer's service
To improve direct marketing

SNCF
TER
To answer customer's demand
To improve customer's service
To improve direct marketing

VDV (Germany)
eTicket Deutschland
To answer customer's demand
To improve customer's service
To improve direct marketing

Västtrafik (Sweden)
To improve customer's service

- **Customer's identity data requested**

ITSO
ITSO card
First Name
Postal Address
Email
Telephone
Gender
Age (or birth)
Other social data

RATP (France)
Navigo
First Name
Postal Address
Email
Telephone
Gender
Age (or birth)
Other social data

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

VDV (Germany)
eTicket Deutschland
First Name
Postal Address
Email
Telephone
Gender
Age (or birth)
Other social data

Västtrafik (Sweden)
First Name
Postal Address
Email
Telephone
Gender
Age (or birth)
Other social data: social security number

- **Personal facts you need to be able to access**

For purchasing of tickets

ITSO (UK)
ITSO card
Single tickets
Multiple tickets
Others tickets
From which point of sale and when the ticket was bought
Information deleted or anonymised : after a period of time

RATP (France)
Navigo
Season tickets
Others tickets
From point of sale and when the ticket was bought
Bank identity
Deletion : 10 years after payment

SNCF (France)
TER
Single tickets
Multiple tickets
Season tickets
From which point of sale and when the ticket was bought
Information deleted or anonymised : after a period of time
Bank identity

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

Deletion : after a period of time

VDV (Germany)
eTicket Deutschland
(only, when personal tickets issued or a subscription contract is agreed)
From point of sale and when the ticket was bought
Information deleted or anonymised : after a period of time
Bank identity

Västtrafik (Sweden)
Single tickets
Multiple tickets
Season tickets
From which point of sale and when the ticket was bought
Information deleted or anonymised : after a period of time
Bank identity

For validations of tickets

RATP (France)
Navigo
Where and when the ticket was validated
Information deleted or anonymised : after a period of time

SNCF (France)
TER
Where and when the ticket was validated
Information deleted or anonymised : after a period of time

VDV (Germany)
eTicket Deutschland
Where and when the ticket was validated
Information deleted or anonymised : after a period of time
Comments : for payment of subscription Tickets or Post-paid entitlements account only in the back office system (it is dependent on the tariff system)

Västtrafik (Sweden)
Where and when the ticket was validated
Information deleted or anonymised : after a period of time

For validations for use of stored value

RATP (France)
Navigo
Where and when each validation occurred

SNCF (France)
TER
Where and when each validation occurred

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

Information deleted: after a period of time

VDV (Germany)
eTicket Deutschland
Where and when each validation occurred
Information deleted: after a period of time
Comment: only in case of autoload

Västtrafik (Sweden)
Where and when each validation occurred
Information deleted: after a period of time

For inspection on board or in stations

SNCF (France)
TER
Where and when each inspection occurred
Information deleted: after a period of time

VDV (Germany)
eTicket Deutschland
Not applicable

6.1.3 Your current organisation for privacy

- **Who stores customers' identity data?**

ITSO (UK)
ITSO card
Collection & Forwarding
Service providers
Customer service providers

RATP (France)
Navigo
Media owners and retailers
Application owners and retailers
Product owners and retailers
Service operators
Customer service operators

SNCF (France)
TER
Media owners and retailers
Application owners and retailers
Product owners and retailers

VDV (Germany
eTicket Deutschland
Media owners and retailers

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

Application owners and retailers
Product owners and retailers
Service operators
Customer service operators

- **Who can access customers' identity data and for what usage?**

ITSO (UK)
ITSO card
Service operators
Customer service providers

RATP (France)
Navigo
Media owners and retailers
Application owners and retailers
Product owners and retailers
Service operators
Customer service operators

SNCF (France)
TER
Media owners and retailers
Application owners and retailers

VDV (Germany
eTicket Deutschland
Media owners and retailers
Application owners and retailers
Product owners and retailers
Service operators
Customer service operators

- **What types of personal data are stored on the card?**

Identity data

ITSO (UK)
ITSO card
Age (or birth)

RATP (France)
Navigo
None (Personal data are only stored on the back office system)
Validations (in and/or out): date, place

VDV (Germany)

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

eTicket Deutschland
First name & surname
Gender
Age (or birth)

Västtrafik (Sweden)
Validations (in and/or out): date, place

- **Transport transactions may occur between the customer and retailers or service operators : how are transport transaction data exchanged?**

ITSO (UK)
ITSO card
Directly from the original retailer or service operator to only concerned actors
Through one of the actors acting as a trusted party for Collection and forwarding
Via a trusted third party appointed for Collection and forwarding

RATP (France)
Navigo
Through a central data base freely accessed by all the IFM Stakeholders

SNCF (France)
TER
Directly from the original retailer or service operator to only concerned actors
Through one of the actors acting as a trusted party for Collection and forwarding
Via a trusted third party appointed for Collection and forwarding

VDV (Germany)
eTicket Deutschland
Through one of the actors acting as a trusted party for Collection and forwarding
Via a trusted third party appointed for Collection and forwarding

Directly from the original retailer or service operator to only concerned actors
No interconnection with unemployed persons files

Västtrafik (Sweden)

Directly from the original retailer or service operator to only concerned actors

- **How is managed the cohabitation of different information management systems for various operators on the same media?**

ITSO (UK)
ITSO card
By segmenting various zones on the media
By sharing the access to information

RATP (France)
Navigo

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

By sharing the access to information

VDV (Germany)
eTicket Deutschland
By segmenting various zones on the media

Västtrafik (Sweden)
By segmenting various zones on the media
By sharing the access to information

- **If you anonymise data :**

Are the hash code keys periodically changed?

SNCF (France)
TER
1 month

VDV (Germany)
eTicket Deutschland
Not applicable

What usage do you do of anonymised transport transaction data?

SNCF (France)
TER
Commercial usages

VDV (Germany)
eTicket Deutschland
Blocking of tickets/entitlements

Fraud control:

Which measures are implemented to fight technological fraud?

ITSO (UK)
ITSO card
Measure 1: SAM
Measure 2 : central security management
Measure 3 : cryptography

VDV (Germany)
eTicket Deutschland
Measure 1 : asymmetric and symmetric authentication between medium and reader
Measure 2: access conditions only for data owners
Measure 3 : monitoring of different counters and data

Västtrafik (Sweden)
Measure 1 : secret write and read access keys

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

Measure 2: encryption of data content on card
Measure 3 : monitoring of transaction patterns

Which measures are taken in case of payment incident?

ITSO (UK)
ITSO card
Measure 1: hotlist

RATP (France)
Navigo
Measure 1: card chip temporary invalidation

VDV (Germany)
eTicket Deutschland
Measure 1: blocking of tickets/entitlements

Västtrafik (Sweden)
Measure 1: customer asked to contact customer services

Which measures in case of usage fraud (for ex, use in a non subscribed zone)

ITSO (UK)
ITSO card
Measure 1: hotlist
Measure 2 : use denied by validator
Measure 3 : manual inspection

RATP (France)
Navigo
Measure 1: penalties for faulty behaviour

VDV (Germany)
eTicket Deutschland
Measure 1: penalties

Which measures in case of suspicion of use of a card belonging to someone else?

ITSO (UK)
ITSO card
Measure 1 : manual inspection
Measure 2 : photo image printed on the card

RATP (France)
Navigo
Measure 1: identity control

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

VDV (Germany)
eTicket Deutschland
It is allowed in most cases (not for personal tickets)

6.4 Solution

- **What data do you expect needing to share in the future with other commercial stakeholders (phone operators, etc.)**

ITSO (UK)
ITSO card
Personal facts related to Payment transactions

RATP (France)
Navigo
Identity data
Personal facts related to Transport transactions
Personal facts related to Payment transactions

SNCF (France)
TER
Identity data
Personal facts related to Transport transactions

VDV (Germany)
eTicket Deutschland
Identity data
Personal facts related to Transport transactions
Personal facts related to Payment transactions

Västtrafik (Sweden)
Personal facts related to Transport transactions
Personal facts related to Payment transactions

- **Is there another solution to be envisioned in place of transport transaction data anonymisation ?**

ITSO (UK)
ITSO card
Comments : card id number is encrypted in transaction data

VDV (Germany)
eTicket Deutschland
Not applicable

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

- **What should be the time length for transport transaction data to be conserved as personal facts?**

ITSO (UK)
ITSO card
For card bearer: 2 years
For transport operators: 2 years

RATP (France)
Navigo
For card bearer : time needed to prove that actual use of transport is covered by contract
For transport operators: time needed to make sure traveller uses transport in conformity with contract

VDV (Germany)
eTicket Deutschland
Not applicable

Västtrafik (Sweden)
For card bearer: 18 months
For transport operators: 365 days

- **Outside payment issues, would your requirements be satisfied if the consumer was only identified via a pseudo and his real identity only accessible on special formal conditions from one or some trusted third parties?**

ITSO (UK)
ITSO card
Yes

RATP (France)
Navigo
No
Comment: not as long as RATP is filling more than a transport operator role

SNCF (France)
TER
No

VDV (Germany)
eTicket Deutschland
Yes
Comment : Core application supports this!

Västtrafik (Sweden)
Yes

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

- **If yes to previous question, would you accept a stakeholder inside your IFM to be one of these trusted third parties?**

ITSO (UK)
ITSO card
Yes

VDV (Germany)
eTicket Deutschland
Yes
Comments (if any): this is the product retailer

- **Do you see any reason for which the card issuer cannot be appointed as such a trusted third party ?**

ITSO (UK)
ITSO card
No

RATP (France)
Navigo
No
Comment: but no reason to take them as a trusted third party more than another partner

SNCF (France)
TER
No

VDV (Germany)
eTicket Deutschland
Yes
Comments (if any): this is not his business

6.5 Results analysis

The 5 public transport organisations play multiple roles within IFM: application owner/ retailer, product owner/retailer, media owner/retailer as well as controller and processor.

The objective for gathering customer personal data is to better answer his/her demands, to improve services, to improve direct marketing. A rather complete scope of personal data (first name and last name, postal address, email, telephone, gender, age, other social data) is requested when the ticket is purchased, validated, for inspection purpose and fraud control. If service providers store them, all IFM categories manage to have access to them.

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

Personal data stored on the card are usually first name, last name, age, gender, but they can also be none in some case. Information is deposited on the card to fit various applications. As transaction data being are shared and exchanged, all kinds of system configuration are used: centrally processed, distributed, given to a third party. When anonymisation is done, hash code is usually changed once a month

To fight technological fraud, control is concentrated on SAM, in the central system and relied on cryptology. Hotlists are used to limit payment incidents. Requested time to keep transaction data is 2 years. Third party role is a litigious issue: some organisations are against it and others are for it.

In a first and provisional conclusion, we can state that, as soon as a common transit application must be shared between different IFM schemes, there is a need to raise consciousness among organisations partners of IFM networks so they identify risks of undue dissemination of customer personal data through data exchanges with other operators as well as because of piracy acts.
There are rules to be respected in order to influence protection level and which are linked with :
- systems where personal data are recorded : fare device, single back-offices, common back-offices,
- access conditions (none, pin code, cryptography),
- exchange conditions,
- actors dealing with personal data.

An IFM actor cannot disclose customer related information to third parties without specific authorisation from the customer. There is an option consisting in setting up a trusted third party which can gather and keep customer's personal data at other IFM actor disposal, provided they have the right to do so. Instead of multiplying and duplicating personal data files (each for one application) as it is frequently the case, the effort should be put on defining specific roles for personal data handling stages from production to exploitation phases with specific responsibilities being attributed to defined IFM actors such as a personal data manager to be added to the overall IFM architecture.

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

Annex 1:

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

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

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.

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

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-I-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

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

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:

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

- 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.

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

Annex 2:

Privacy Policy in UK

Keeping Your Data Safe

We take the privacy of client and end user data very seriously. Any personal data collected by a client using the eTickets.to service, or disclosed to us during the use of our service is the property of that client. We will only process such data to the extent necessary to provide the eTickets.to services.

We will never sell, rent or disclose client data without the express written consent of a client, unless we have a legal obligation to do so.

That's the short version. Because our lawyers like to earn their fees, they insisted that we also have the long version below...

e-Ticketing Technologies LLP (referred to in this Privacy Policy as "eTickets.to", "we", "us" or "our") is committed to protecting your privacy. This Privacy Policy explains how we use the information we collect about you through eTickets.to, how you can instruct us if you prefer to limit the use of that information and procedures that we have in place to safeguard your privacy. This Privacy Policy forms part of the Terms of Use

1. Contact details

The eTickets.to website (the "Site") and the eTickets.to ticketing services (together, the "Services") are provided by e-Ticketing Technologies LLP, a partnership registered in England and Wales with company registration number OC317780.

Registered Office: e-Ticketing Technologies LLP, 60 Maltings Place, Fulham, London SW6 2BX, UK. **Contact Address:** 60 Maltings Place, Fulham, London SW6 2BX. **e-mail:** hello@etickets.to

2. Introduction

2.1 We are registered under, and process personal data in accordance with, the United Kingdom's data protection laws.

2.2 This Privacy Policy covers the provision of the Services only and not any other companies' websites which you may access from the Site or by using the Services. 2.3 If we change the Privacy Policy we will place notices on the Site and post the changes on this page. If you do not accept any changes to the Privacy Policy please stop using the Services and close your membership account.

3. Personal Information Collected

3.1 We will only collect personal information about you that you have given, either:

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

(a) when you register to use the Services to sell tickets (as a 'Client'); or (b) when you make a purchase using the eTickets.to system (as a 'Customer'. 3.2 When you register to use the Services or make a purchase you will be asked to provide personal information such as your name, e-mail address and contact telephone numbers.

4. Use of personal Information

4.1 If you register as a Client we may use personal information for: administrative, operational and marketing purposes and to communicate with you about your use of the Services any changes to the Services. We will only pass on your information to other companies if it is necessary to perform the Services or with your prior consent. Those companies may contact you to inform you of their services and products. Any personal information that you choose to provide to us or to other companies using our Services will only be used in support of the intended purposes stated at the time at which it was collected and subject to any preferences indicated by you.

4.2 If you make a purchase through the eTickets.to system we will use your details solely for the purposes of processing your order and to service any support requests you make. We will pass your data on to the Client you are purchasing from, who will have their own Privacy Policy which will apply. We will not sell or rent your data. We will not disclose your data to third parties except to the extent required to fulfil your order and meet our legal obligations.
4.3 If you breach the Terms of Use your personal information may be passed to third parties, such as our legal advisors to the extent necessary to enable those third parties to resolve the matter.
4.4 If this business is sold or integrated with another business, your details may be disclosed to our advisors and any prospective purchasers and their advisors and will be passed on to the new owners of the business.

4.5 We may be obliged to disclose your personal information if required to do so by law.

5. Other Information

5.1 We may also collect and disclose information to third parties in aggregate (so that no individual members are identified) for statistical analysis and strategic development purposes.

6. Cookies

6.1 We may use "cookies" to collect aggregate information. A "Cookie" is a small piece of information sent by our web server to your web browser, which enables us to record anonymous details and allows you to move around the Site faster. We may use cookies for a number of purposes, for instance to enable us to simplify the logging on process, to help ensure the security and authenticity of members and to enable traffic monitoring. You can find out more about the way cookies work on http://www.cookiecentral.com.
6.2 Most browsers allow you to turn off the cookie function. If you want to know

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

how to do this, please look at the help menu on your browser. However, if you turn off the cookie function your use of the Services may be impaired.

7. Overseas

7.1 We will only pass on information about you as an individual (as opposed to aggregate information) to third parties overseas to enable us to perform services requested by you.
7.2 Owing to the global nature of the Internet, the information you provide may be transferred in transit to countries outside the European Economic Area that do not have similar protections in place regarding your data and its use as set out in this policy. However, we do our best to ensure that your personal information is secure.

8. Security

8.1 As required by under UK data protection laws, we follow strict security procedures in the storage and disclosure of information which you have given to us, to prevent unauthorised access. We use industry standard technology to encrypt your personal information. However, the Internet is not a secure environment and we cannot guarantee the security of any information which you send to us.

9. Other websites

9.1 Our Site may contain links to other websites which are outside our control and are not covered by this Privacy Policy. If you access other websites using the links provided, the operators of these websites may collect information from you which will be used by them in accordance with their privacy practices, which may differ from ours.

10. Updating your details

10.1 If you wish to update any of your personal details at any time, for example if you change your e-mail address, or you do not wish to receive information about a particular product or service, or if you wish to close your account, please email us at hello@etickets.to

11. Access rights

11.1 You have a right to access the personal data that is held about you. To obtain a copy of the personal information we hold about you, please write to: Privacy Officer, e-Ticketing Technologies LLP, 60 Maltings Place, London, SW6 2BX, UK, enclosing a cheque for £10 payable to e-Ticketing Technologies LLP to cover our administration costs.

When writing to us, please state your name, postal address and mobile phone number and provide brief details of the information that you require.

12. Contact us

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

If you would like to contact us with any queries or comments on our privacy practices, please write to the contact address above or send an e-mail to hello@etickets.to

http://www.etickets.to/privacy.html

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

Annex 3 :

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

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

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

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

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

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

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,

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

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

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

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 trough 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

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

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

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

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

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

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).

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

[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. Taetigkeitsbericht 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).

[59] Homepage at [link].

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

[60] Munich Atlas at [link].

[61] Homepage at [link].

[62] Stefan Krempl, "Urteil schränkt Videoüberwachung 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