

ANNEX 1 ISO 24014

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.
Customer service	Subject to commercial agreements <u>may</u> provide “helpline” and any similar facilities including stolen and damaged Customer Medium replacement and consequential Product reinstalling.
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.
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: <ul style="list-style-type: none">○ 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: <ul style="list-style-type: none">○ 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.

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 Entity 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.

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.

Complement

The above IFM model is independent from the media which host the applications inside which the products are stored.

In most of the current use cases, where only one card is issued, the application owner is also the issuer and the owner of the media.

As multi-application media develop, the complete description of the framework of the system should include two new functions:

Medium Owner

Holds the Contract for the use of the medium with the customer.
The medium owner also holds the contracts with the application owner to install the application inside his medium.

Medium Retailer

Sells the medium to a customer.
The medium Retailer is the financial interface between the customer and the medium owner.

ANNEX 2 European recommendations:

Full text can be downloaded at:

http://www.datenschutz-berlin.de/attachments/335/e-ticket_en.pdf

A so-called “G29 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.

The Working Party 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.

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

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

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

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

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

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

Privacy Impact Assessment

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

Anonymity

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

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

Privacy Policy and Transparency

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

Data Minimization and Retention Period

As regards, in particular, processing of the data concerning users' movements, the information systems of transport companies should be designed and implemented by prioritizing the use of anonymous data. If (directly or indirectly) identifiable information is used, this information should be stored for the shortest possible period (and erased automatically thereafter), and account should be taken of the lawful purposes to be achieved via the processing – as a rule, the information in question should not be retained for longer than a few days after being stored.

Security

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

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

Marketing

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

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.

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.

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.

ANNEX 3 Definitions of terms used in the questionnaire

In this questionnaire, please consider these definitions.

Personal data

Any information concerning an identified or identifiable natural person. Personal data include identity data and personal facts (see below).

Identity data. It includes :

- *“Direct” data : first name, last name, date and place of birth...*
- *Transport “Indirect” identity data: card ID...*
- *Bank “indirect” identity data: account number, etc.*

Personal facts

Every fact concerning an identified or identifiable natural person (also referred to as “personally identifiable information”).

Personal facts include:

- *Transport transaction data: types of ticket, places where tickets are bought and used, etc.*
- *Payment transaction data: purchase operations, etc.*

Anonymisation

“Anonymisation” is the action of converting a personal fact into a pseudo-personal fact. Pseudo-personal facts make impossible any backtracking from the facts to the individual person. But they can be processed to link the facts together to investigate (anonymous) customer behaviours.

Hash functions

Hash functions are mostly used for “anonymisation”. They use a non-reversible algorithm to replace the identity data by a pseudo processed from a hash key.

(Definitions discussed in the Forum to be added later).