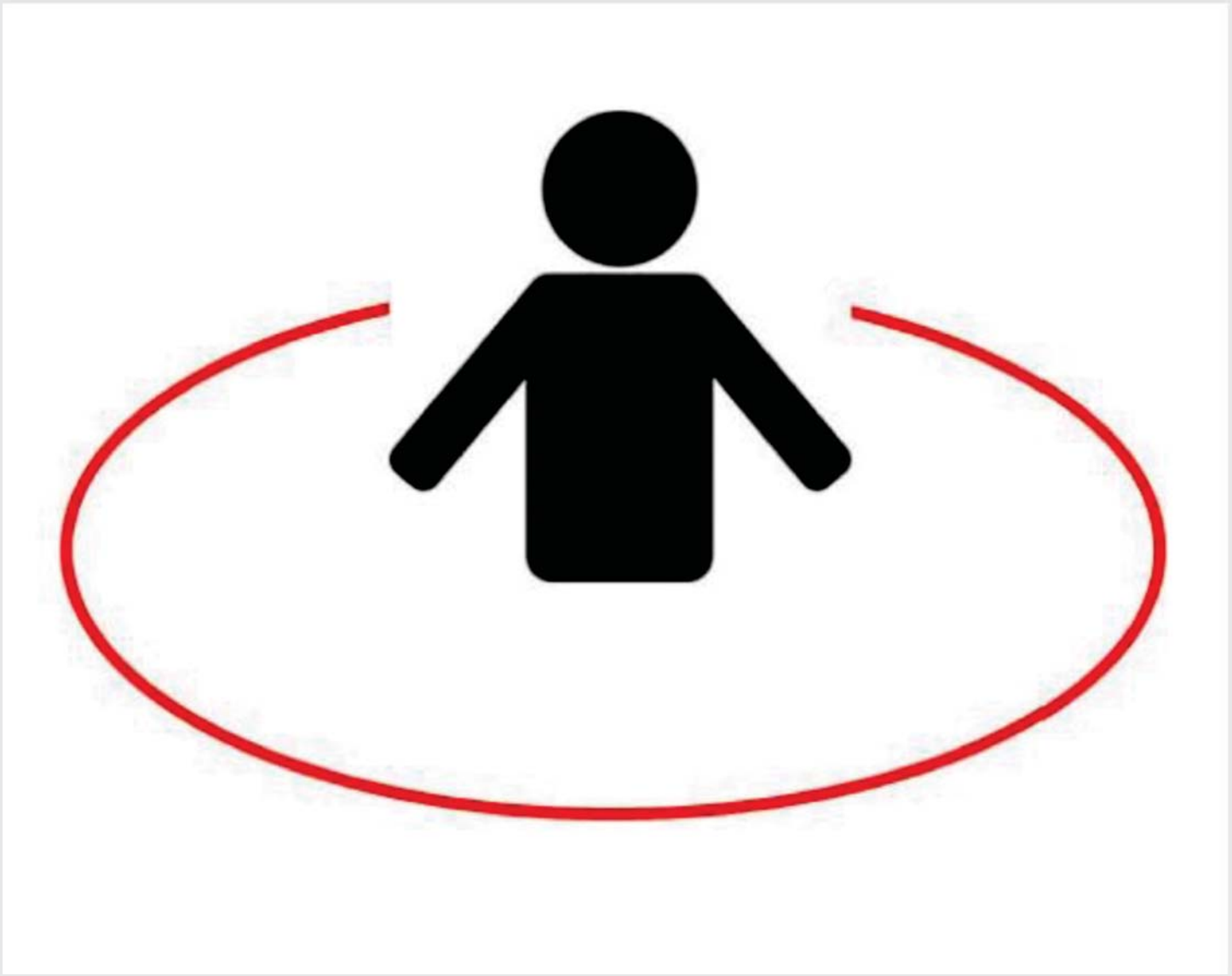
Directorate of Public Roads
Roads and Transport Department
Traffic Management Section
2014

Statens vegvesen

# The Industry Standard

## On the right of privacy and information security in electronic ticketing



Trond Foss

Revision history

| Version | Date | Autors | Important changes |
|---|---|---|---|
| 1 | December 2011 | Eva Jarbekk, Svend Eric Wandaas, Mette Hendbukt | First version of the document |
| 2 | September 2014 | Mette Hendbukt, Eva Jarbekk, Cathrine Ruud | New front-page, clarification of privacy-by design, new paragraph regarding mobile ticketing (chapter 7.9.2) |

# Content

# 1 Background and objective

The industry of public transport in Norway is in the process of implementing solutions for electronic ticketing. The implementation of these solutions is a political goal and some companies have already introduced electronic ticketing. But the majority are still in the planning stage. *The political goal is to enable seamless travelling in Norway, by using electronic tickets regardless of which carrier is being used.*

The introduction of electronic ticketing raises some issues regarding the law of privacy protection. These have to be solved in pursuance of Act of 14 April 2000 no. 31 relating to the processing of personal data [Personal Data Act] (**POL**) and accompanying regulations. The Personal Data Act is based on EU-Directive 95/46/EC, i.e. on the protection of individuals concerning the processing of personal data.

This industry standard is prepared due to a need to have a mutual understanding of how to interpret the legislation. This standard is prepared by principal stakeholders/participants in this industry, Transport authorities and the Norwegian Data Protection Authority together. The objective is to create predictability for the stakeholders regarding the interpretation of the legislation, and to create a confidence-inspiring and reliable protection of privacy for the travellers.

# 2 The relation between the industry standard and other regulations

The industry standard is sanctioned by the law POL Section 42, third paragraph (6).

All companies that have permits or receive grants are obliged to follow NPRA Manual V821. Manual V821 refers to this industry standard and hence it is (legally) binding for all stakeholders.

Companies that are not obliged to follow NPRA Manual V821 may choose to affiliate with the industry standard, informing the Directorate of Public Roads of this in writing. The Directorate is responsible for maintaining a record of these enterprises. The standard sets out basic principles for electronic ticketing, but is not exhaustive. Each company is obliged to ensure that the

legislation is observed and that statutory internal control systems are prepared to take care of this.

The industry standard applies with exceptions of nonconforming national and international legal obligations.

# 3 Processing personal data in public transport

The design of the electronic ticket concepts are based on Manual V821 which has been prepared by the Directorate of Public Roads in the NPRA and stakeholders in the industry.

The electronic ticketing systems are based on transactions, i.e. that the structure of systems depends on the collection of travel information for each individual transaction in order to fulfil certain intentions of the processing, see Annex 1[1]. Manual V821 is based on ISO/DIS 24014-1:2005.

The agreement between the traveller and the transporter is stored on the electronic travelcard. The rights of the individual traveller are recorded in a "*contract"* on the travelcard. The contract is displayed in the card-reader, which normally generates a transaction and collects the travel information described in Annex 1. Many of the systems are off-line and a non-synchronous data transmission takes place.

The card-number, together with a transaction-counter on the card, is essential in the electronic ticket systems. The card-number is necessary in order to verify that all card-readings have been registered and are correct. For example, the card-number is crucial in order to be able to debug and verify that relevant transactions (sales, validations, refunds etc.) are included in the statement of accounts.

Besides, the card-number will be crucial in order to be able to render additional service to the customer, e.g. subscription and reconstruction of transactions.

Some travellers have an agreement including different varieties of a travel-account. These agreements involve a payment commitment stored on the card – synchronized with a payment instrument in the back office system. An

[1] The annexes are not translated, contact NPRA for more information

account number may only be used when such an agreement with a customer is entered into in advance.

Not all activity results in an accumulation or storage of travel information when using the ticket medium on a ticket machine. One example of this will be when a customer just wants to check which product is stored on the card, or if it is valid.

# 4 Data Protection Officer (DPO)

It is recommended that the companies appoint a DPO to assist them and the customers with questions of privacy and also follow up internal control.

# 5 Consent and requirement for anonymous alternatives

The customer has a fundamental right to be able to control his/her own personal data and to choose to move around anonymously in the society. The use of personal data in electronic ticketing has to be based on a legal consent from the customer, cf. POL Section 11, first paragraph, (a) and Section 8, first paragraph.

This needs to be an explicit, voluntary and informed consent. The voluntariness is considered genuine only when anonymous alternatives to personalised travel products are available.

The ability to move freely around in a democratic society without having one's movements recorded, is considered to be an important part of our private lives, cf. Article 8, (1), of The European Convention on Human Rights, Article 17 of the UN International Covenant on civil and political rights, and Section 2 of The Norwegian Human Rights Act.

The companies are hence obliged to offer anonymous alternatives in addition to personalised tickets and services.

Below is a description of how a company should offer anonymous alternatives, so that the anonymous alternative constitutes an eligible alternative for the traveller.  A registered card that is not registered in the name of the possessor, is regarded as sufficiently anonymous[2].

[2] This implies that a card with photo and name is considered anonymous as long as it cannot be identified by the card issuer.

### 5.1 Price

Anonymous and registered travels shall be offered at the same price.

For all essential personalised travel products there must be corresponding anonymous products available. But it is not required to offer exactly the same type of product as long as the anonymous alternative is at least as advantageous for the customer as the personalised ticket. Thus, if a discount scheme is offered, equal discount schemes have to be offered for both personalised and anonymous products.

### 5.2 Sales channels

As a rule, products that allow the buyer to travel anonymously, must be available for sale through the same sales channels as the personalised products. This includes sales channels where tickets can be bought over the counter and from automatic vending machines.

If a product is sold through an internet application, this application also has to include anonymous products, and it must be possible to carry out the purchase anonymously.

Exceptions from this rule may be made if it is not feasible to offer anonymous products for practical reasons, as long as an alternative sales channel is being offered which is easily accessible.

### 5.3 Supplementary services

Supplementary services that are not tied to the right to travel, may be personalised. Examples include SMS-notifications when delays occur, and deferred payment.

As far as possible, reconstruction and reimbursement for lost cards ought to, be offered anonymously, also when implementing new solutions, revisions, (further) development or changes.

## 6 Right of access

### 6.1 General right of access

Everybody can claim the right of access to the following information:

a. Name and address of data controller, typically the name of the company and address. The information must also specify who has the everyday responsibility for ensuring that the company complies with the law.
b. The company has to be able to give an account of the purpose of their processing of personal data and what type of personal data that are being processed, see Chapter 8.
c. It is required to specify where the information derives from, and whether it will be forwarded and if so to whom.
d. The right of access according to The Freedom of Information Act (FIA) does not include access to travel information, cf. FIA Section 13, second paragraph and Public Administration Act Section 13, first paragraph (1).

As far as possible, non-registered customers have the right of access to travel information on the card at their disposal to be able to control its functionality and transactions, as well as the right to complain if errors occur.[3]

## 6.2 The right of access for registered customers

In addition to what is detailed in chapter 6.1, registered customers may request to know what kind of information is actually recorded about themselves.

The company needs to prepare internal procedures ensuring that only the person about whom information is registered is given access to this information. These procedures are to be based on the following principles:

- The payer has the right of access to information concerning the actual purchase only.[4]
- The registered owner of a card has the right of access to all information about himself/herself that is being processed.
- To simplify the procedure and if agreed upon with the purchaser, access may, be limited to the most relevant information such as what customer-information that is registered and travel-information specifying the time and place of the actual journey.

[3] This may be done for instance by allowing access when displaying the card

[4] This entails that the time and place of a journey cannot be given

- The registered owner has also the right of access to the security measures tied to the processing in question.

Companies are to describe such security measures in a separate document made accessible for distribution. This applies only if such access does not undermine the security. It is sufficient for instance to use a designation of the relevant security measure, like stating that the cards are protected with “DESFire” technology without describing the security solution in detail.

### 6.2.1 How access is to be granted

In order to get extended access to what kind of information is being processed, the request must be made either by personal attendance, in a signed letter, or by email. The person making the request must be identifiable as the registered person.

The reply will be sent by regular mail to the address that is registered and not by email.

As an alternative, access may be given through electronic facilities, for instance using a “MyPage” solution.

As a rule, access to process-related comments will not be given. These are considered to be text prepared for internal use only.

### 6.2.2 Time limit for replying to an inquiry

Replies to inquiries about access, are to be given without undue delay and no later than 30 days from receipt of the inquiry. If, for some reason, the reply will take more time, a preliminary reply has to be given stating the reason for the delay and when a reply is likely to be given.

## 6.3 Rectification of existing information

The company has an obligation to correct erroneous information about the registered person. The main goal with this correction is to make sure that the company has updated and correct information about the customer.

The company has an obligation to make sure that the information being processed is correct. Thus the company must see to it that the necessary updating and correction of information takes place. If there is doubt about

the correctness of the information, it must be verified, for instance by contacting the customer.

Rectification should be carried out as soon as possible after an inquiry from the affected customer, unless the company has reason to doubt that the inquiry is coming from the right person or that the new information is correct.

Rectification implies normally that incorrect information is deleted. However, the requirement regarding updating and rectification of information, does not imply deleting information that is essential as documentation, e.g. in a case about ticket inspection. Updating will then take place by highlighting the old information and supplementing them with the correct information.

# 7 Basic requirements regarding the processing of personal data in the e-ticketing system

## 7.1 Consent and other basis for processing

There has to exist legal grounds for processing, covering each purpose for which the personal data is being used. The following subchapters present a review of relevant legal grounds for processing.

### 7.1.1 Requirement as to form – some general particulars about consent and information to the customer

Consent is given by the customer based on the information the company has presented. Consent has to be voluntary, cf. Chapter 5 regarding anonymous alternatives.

Consent may be given verbally, but for the sake of verification, it is strongly recommended that it is given in writing or by using a check box on an electronic form.

If the payer is another than the person holding/using the card, the payer must ensure that the person concerned is given sufficient information.[5]

Consent and information must include the following as a minimum:

- Who is responsible for processing personal data
- Information declaring that consent is voluntary and that anonymous alternatives exist.
- The purpose of the processing is to be stated, see Annex 1. Typical examples:
    - To issue tickets, for instance by automatic renewal of ticket or "travel money" (pay-as-you-go credit)
    - To provide passenger service by offering supplementary services like:
        - Reconstruction of transactions
        - Refund of significant amounts
        - SMS notification
    - To perform troubleshooting and internal control
    - To settle invoice documentation between companies (interconnection between travel information and personal data may not take place).
- Information about when and to whom personal data is revealed.
- What type of information that is collected, is to be specified in detail; typically as personal data (basic data such as name, address etc), travel information including the detailing level regarding time and place of use, journey history, and sales information.
- Storage time for data.
- Information regarding the right to demand access, correction and deletion of incorrect information.

Annex 2 presents a template for how consent and information may be formulated. The template is based on the objectives the industry typically has for basic travel products and supplementary services.

[5] Typically this is applicable when an employer pays for a travel card for use during office hours by the employees. For the employees to use registered cards, consent is required from each employee.

The company is obliged to guide their customers in how to carry out a reading which does not involve collecting or storing travel information, for example when the customer only wants to check the content on the card.

### 7.1.2 The use of personal profiles

In order to give the customer customized offers and information based on the customer's use, the customer must give his/her consent specifically for this. Annex 2 shows a template for how such consent may be obtained.

When communicating with a customer, he/she must be specifically informed as to what information is the basis for the inquiry and where it has been obtained.

### 7.1.3 Direct marketing in existing customer relationship

According to the Marketing Control Act Section 15, third paragraph, it is permissible to carry out direct marketing towards registered customers, unless the customer in advance or when receiving offers and information reserves the right to refuse. The customer must be given the opportunity to easily reserve the right to refuse any inquiry or attempt at collecting information.

### 7.1.4 Ticket inspection – protecting a legitimate interest

Customers that cannot present a valid ticket will have to pay an additional charge fee according to Section 33 of the Professional Transport Act and the companies own transport statutes.

The companies are considered to have a legitimate interest to process personal data about customers who cannot present a valid ticket upon inspection. The purpose of the processing is to ensure a legitimate and efficient collection of the surcharge.

### 7.1.5 Ensuring school transport

School transport is a right for pupils, on certain conditions as specified in the Education Act, Chapter 7. The county authority in some cases delegates the power to their own administration enterprise, which requires entering into a Data processor agreement. If such an agreement is in force, then the processing of sensitive data regarding health issues is exempt from the

license requirement according to POL, Section 33, fourth paragraph, because the processing has legal grounds in the Education Act, Chapter 7.

The purpose of the processing of personal data is to exercise public authority and provide school transport for pupils on the right basis. It may be necessary to use national identity numbers in order to obtain reliable identification.

Special transport is granted to pupils who are entitled to school transport due to health issues.

### 7.1.6 Other purposes

Personal data that are collected for the above-mentioned purposes, cannot be used for other purposes without specific legal grounds, cf. POL Section 11, first paragraph.

## 7.2 Legitimate purposes

The processing of personal data in public transport may only be initiated in order to achieve what is, considered legitimate for the operation of the company, according to POL Section 11, first paragraph (b).

All purposes that are listed above and in Annex 1, are regarded as legitimate for the activities the company is pursuing.

## 7.3 Relevant information

The type of information being processed, must be relevant for the purpose at hand, cf. POL Section 1, first paragraph, letter (d).

The types of information described in relation to the individual purpose in Annex 1, are considered relevant for this particular process.

The processing of the card number is considered relevant for the attainment of most of the purposes designated in the present industry standard Chapter 7.1.1, fourth paragraph and in Annex 1. For the processing of personal data on customers that have entered into an agreement for a travel account, the processing of the travel account is also considered relevant for the follow-up of the use of such a travel account.

The processing of national identity numbers is considered relevant in order to exercise public authority according to the specifications in the industry standard Chapter 7.1.5, cf. POL Section 12. For the same reason, health-information is considered relevant as long as it is essential in order to authorize transport on medical grounds according to the Education Act, Chapter 7.

The companies comprised by this standard are obligated not to start the processing of other types of information for alternative purposes without this having been assessed and approved in accordance with the routines for alterations in the industry standard (Chapter 10) in advance.

## 7.4 Storage and elimination of personal data

Information that is no longer needed is to be deleted. Elimination of travel information may be carried out by deleting all the information physically, or by deleting/replacing the card-number in an irreversible manner. Travel information is in all cases to be deleted/anonymized after 104 days.

Customer information may be stored as long as the customer has a customer-relationship with the company. If the customer withdraws his/her consent, the card must not be blocked or handed in before any valid ticket on the card has expired or is expended. In cases where the customer withdraws his/her consent and either hands in the card or gets the card depersonalized, the personal data are to be deleted within 14 days of the termination of the contractual relationship. The customer is to receive clear information on how this may be carried out.

Information needed for invoice- or filing-purposes, has to comply with special rules, see Annex 5.

To make sure that the above-mentioned deadlines for erasing information are observed, all companies are to prepare routines for how to delete information in all the data bases and files where personal data are stored. Documents containing personal data are to be obliterated in a secure way.

When it comes to deleting unnecessary personal data, the situation is to be described in a yearly information review, in order to obtain a management's evaluation of the companies' security objectives and strategy, cf. Personal Data Regulations, Section 2-3.

## 7.5 Access to personal data

Only those employees working in the companies, who have a legitimate need to access personal data and/or travel information, are to have access to those parts of the electronic ticketing system where this information is stored.

The data controllers' employees are to be pledged to confidentiality with regard to personal data and other information significant to information security.

Logs are to be kept that show who has made use of the information system. In addition, an account is to be kept of all authorized users of the application that allows access to personal data.

## 7.6 Settlement of accounts between companies

Some companies have established concepts where the traveller may use a travel product issued by one of their collaborating companies. In order to settle accounts correctly between the companies, it is necessary to process information regarding *which* products are used and *where*.

When settling such accounts, it will not be necessary to identify who has actually made the journey. The companies are to make sure that whoever is performing the settlement of accounts will not be able to access information that will make it possible to connect the owner of a product with the completed journey. This is to be solved by allowing the companies to reveal only the card number and its use, and by entering into a Data processor agreement with the company performing the settlement of accounts.

## 7.7 Revealing personal data to other people than the customer

### 7.7.1 Principal rule

It is a requirement that there exists legal grounds for handing personal data over to a third party. The customer is to be informed when and to whom the information will be forwarded.

### 7.7.2 Forwarding to the police or the prosecuting authority

The court may rule that the company is to reveal personal data if these are presumed to be of importance to an ongoing case, cf. the Criminal Procedure Act, section 210, first paragraph.

If there is danger that the investigation will be impaired as a result of having to wait for the court's decision, the police may request an order from the prosecuting authority to have the information surrendered, cf. the Criminal Procedure Act, Section 210, second paragraph. The decision of the prosecuting authority has to be submitted to the court for approval as soon as possible.

When an information surrender-order is issued, the company will have to demand a copy of the court's ruling or the prosecuting authority's written instructions.

## 7.8 The use of data processors

If the company employs external service providers, partially or entirely, to process personal data, the company has to enter into a Data processor agreement with the external provider.

As a minimum, the Data processor agreement is to specify the purpose and basis for the processing, describe how the information will be processed, govern the use of sub-providers, ensure the rights of the person to whom the information pertains, and instruct the provider to have a satisfactory information security. Annex 3 describes how the Data processor agreement may be formulated and followed up.

The company has to establish procedures ensuring that the provider implements the processing according to the agreement.

## 7.9 The use of new concepts and technology

New concepts and technology that may contribute to improve public transport, are continuously emerging. The use of new technology or new concepts is to be assessed with regard to the principles in the Standard, when it comes to the consequences of privacy protection as well as to questions regarding information security. The assessment is to be reviewed

by the Working Group (see Chapter 10.3) as a basis for revision of the Standard, cf. Chapter 10.

To ensure that new technology is utilised in a way that safeguard the prescribed rules and principles of privacy protection, the industry is to base their activities on the requirements mentioned below, and at the same time include the protection of privacy already in the design phases of new products and services, so that the use of personal data is reduced to a minimum (privacy by design).

### 7.9.1 Particulars about internet solutions

The Internet is used increasingly to offer various services. When using the Internet, the company is to safeguard the requirement for anonymity when new solutions are being developed, see Chapter 5.

Anonymity may for instance be undermined in connection with the logging of IP-addresses, the use of cookies etc. When selling or managing anonymous products, such services are not to be based on the logging of IP-addresses or the use of other elements that may undermine the customers' anonymity. This includes the use of third-party devices/equipment or similar.

Brief logging of IP-addresses for security reasons is not considered a threat to anonymity, cf. Personal Data Regulations Sections 7-11 and 2-16.

In solutions and screen interfaces where anonymity is selected, there should be no unnecessary text boxes or other applications that invite the submission of personal data.

It must not be possible for customers who want anonymity to accidently compromise their anonymity by typing identifying information such as name, telephone number or email address in a text box on MyPage when purchasing or managing anonymous products. The system must be adapted so that customers who want anonymity not by a simple mistake undermine their own anonymity.

### 7.9.2 Particulars about mobile ticketing

Solutions using mobile applications.

Before downloading the application, the customer must be given access to information about what kind of data in the mobile phone the application

utilises, why and for what purpose it is used, and what is being stored. This kind of information is to be accessible both where the application is downloaded and within the application itself.

### 7.9.3 Payment methods

When payment methods over the Internet are used, personal data are not to be processed when anonymity is requested, cf. Chapter 5.

This may be solved by separating the payment from the ticketing system.

In cases where the payment is not separated from the ticketing system, then the personal data have to be filtered away as soon as the transaction is completed.

### 7.9.4 The use of email and mobile phone numbers

Email addresses may be used as identifiers in anonymous solutions, but the company ought to inform the customer his/her anonymity may be compromised if the email address clearly shows a name or some other obvious identification.

The company is not to use mobile phone numbers as identifiers in anonymous solutions.

# 8 Data security

## 8.1 Basic requirements

Pursuant to the Personal Data Act, data security is about safeguarding the personal data with regard to confidentiality, accessibility, integrity and quality.

The responsibility rests with the company's topmost executive, who in turn can delegate the execution of the responsibility. Security objectives are to be defined and assessments made as to what constitutes an acceptable security level, and these are to be specified in steering documents in the company's internal control system. Implemented control routines and measures are to secure personal data against misuse both internally and externally, based on a risk evaluation.

### 8.2 Discrepancies from the rules

Any discrepancy from the rules is to be registered and implemented actions are to be documented.

If discrepancy from the rules has resulted in unauthorized distribution of personal data where confidentiality is necessary, the Norwegian Data Protection Authority is to be notified.

### 8.3 Risk evaluations

Risk evaluations are a tool used to ensure sound data security practices. Risk evaluations are to be performed before changes are made to existing solutions and before establishing new ones. Risk evaluations are to assess the probability and consequences of undesirable incidents for the company and for the customer.

As a minimum, risk evaluations are to ensure, that the privacy protection principles and security requirements of this industry standard are observed.

### 8.4 Internal control system

Further development of the documentation and internal control system depends of the actual situation in each company. Regulations regarding this can be found in the Personal Data Regulations Chapter 2. Annex 4 presents a guide to how an internal control system may be constructed. The DPO of the company is to be involved in the work with the internal control system.

## 9 Compliance and inspection

The individual company is responsible for fulfilling the provisions set out in this standard. The Norwegian Data Protection Authority relies on the standard when supervising and inspecting companies that are to comply with the standard.

## 10 Updating and changing the industry standard

### 10.1 Routines for making alterations

The industry standard will have to be updated in accordance with relevant changes in the legal framework, new technology etc.

Revisions are to be approved by a steering committee based on a proposal from a working group. The steering committee's approval will then be formalised as an amendment to the industry standard by the Norwegian Data Protection Authority according to the regulations in POL Section 42, third paragraph (6).

## 10.2 The steering committee

As a minimum the steering committee is comprised of the following members:

- One representative from the Norwegian Public Roads Administration, Directorate of Public Roads
- One lawyer and one engineer from the Norwegian Data Protection Authority
- Representatives appointed by Kollektivtrafikkforeningen (a special interest organisation for the companies)
- One representative from Samferdselssjefskollegiet (a body of all transport leaders in the counties)
- One representative from Ruter – Public transport enterprise in the Oslo region
- One representative from NSB – Norwegian State Railways
- One representative from AtB – Public transport enterprise owned by Sør-Trøndelag County
- One representative from Skyss – Public transport enterprise owned by Hordaland County
- One representative from Interoperability Services Ltd.

The steering committee may, as required, appoint other participants to serve on the committee.

The steering committee should aim at making decisions unanimously.

## 10.3 The working group

As a minimum the working group is comprised of the following members:

- One representative from the Norwegian Public Roads Administration, Directorate of Public Roads
- One lawyer and one engineer from the Norwegian Data Protection Authority

- Representatives appointed by Kollektivtrafikkforeningen (a special interest organisation for the enterprises)
- One representative from Ruter – Public transport enterprise in the Oslo region
- One representative from NSB – Norwegian State Railways
- One representative from AtB – Public transport enterprise owned by Sør-Trøndelag County
- One representative from Skyss – Public transport enterprise owned by Hordaland County
- One representative from Vestviken Kollektivtrafikk AS, Vestfold County
- One representative from Oppland County Administration
- One representative from Interoperability Services Ltd.

If many companies have DPO's, then the Directorate of Public Roads is to appoint at least three DPO's to participate in this group.

More participants may be added as required.

The working group should aim at making decisions unanimously.

### 10.4 Meetings

The working group meets at least once a year in order to discuss the follow-up of the industry standard and the need for revisions. The Directorate of Public Roads calls those meetings.

As required, the steering committee is to get prepared a plan for making revisions of the standard according to initiative from the working group.

## 11 Commencement and interim arrangements

The industry standard came into force on 1 June 2012.

If a company has a legitimate need for technical adaption and/or financing of new solutions in order to comply with the standard, the Norwegian Data Protection Authority may consent to a period of transition on the following conditions:

- The company is to present a work plan that shows what issues the company is actively working with to improve in order to comply with the demands of the industry standard – and
- The work plan is to show clearly the expected progression and what actions are planned in order to meet the industry standard's demands, as well as how long the interim period needs to be.

Some companies currently offer only personalised tickets. During their potential interim period, these companies are to offer, at least one product that to the extent possible fulfils the criterion of anonymity and equal price, cf. Chapter 5.

# 12 Definitions

## 12.1 Legal

**Anonymous information**: Information where name, national identity number and other personally identifiable characteristics are removed or not registered, in a way that makes it impossible to connect the information to the identity of an individual.

**Anonymous (travel) card**: A card that the company is not able to connect to the identity of an individual.

**Processing**: Any use of personal data, such as collection, recording, compilation, storage and distribution or any combination of these uses.

**Legal grounds for processing**: Legal ground needed to process personal data, such as the customer's consent, legislative warrant – or the exercise of public authority.

**Data controller**: The person who determines the purpose of the processing of personal data and which means are to be used.

**Data processer**: The person who processes personal data on behalf of the data controller.

**Data processor agreement**: An agreement that governs the rights and duties between the Data controller and the Data processer.

**Customer data**: Customer data is the contact data concerning the registered person, such as name, address and card number.

**The registered person**: The person to whom the personal data may be linked.

**Personal data**: Any information and assessments that may be linked to an individual person.

**Travel data**: Information on the card from a transaction that is registered when a ticket is used.

**Manual V821**: A guide/standard for electronic ticketing, to be observed by everyone holding a licence to operate public transport according to the Professional Transport Act.

## 12.2 Roles and responsibilities

**Company**: An agency in the county administration or a company that is a member of the Association of public transport and that is planning, coordinating, ordering and marketing the public transport in a county or in a more limited area.

**Customer**: A person who enters into an agreement with a product-owner and/or a Service provider and who normally uses the public transport service him-/herself.

**Card issuer**: The company that has issued the card.

**Product owner**: A company or agency that defines all the products that the product owner will offer to the customer. The product owner is the customer's contracting party, and also responsible for the service providers that have accepted the product owner's travel document as a document that makes the customer entitled to a transport service.

**Service provider**: The company that actually transports the customer.

## 12.3 Tickets and cards

**Anonymous ticket/product**: A ticket that can be used by the bearer without he/she having to reveal personal data to the company as long as the customer has a valid ticket.

**Ticket**: Documentation showing the right to travel/customer contract regarding public transport stored on a ticket medium.

**Valid ticket**: Activated ticket giving the customer the right to travel the relevant distance. The criteria for what is considered a valid ticket, are established in detail in the particular company's terms for travelling.

**Card**: A ticket medium that may consist of both tickets and "travel money".

**Card number**: A unique identifier of the card, stored both on the card and in the back office system.

**Period ticket (a period of one day up to one year)**: A ticket enabling the customer to travel between certain areas or distances during a certain time interval, for instance 30 days after being activated.

**Personalised ticket**: A ticket that is stored on a personal card and that can only be used by the registered owner of the card.

**Registered card**: A card where the information about its owner is recorded in a customer register.

**Travel account**: An account that is centrally stored by the company and that is charged according to agreement every time the customer uses the account to pay for a ticket.

**Travel account number**: The agreement number of a travel account stored on the card.

**Travel money**: The value stored on the card that can be used to pay for a journey or buy a ticket.

**Personalised card**: A card that is registered on or issued to one particular individual.

**Non-registered card**: A card where information about the owner is not recorded in a customer register.

## 12.4 Certain actions to be made with the card/device

**Activate the ticket**: Start a ticket embedded in the card.

**Automatic top-up**: Regular adding of travel money on the card according to the agreement with the customer.

**Ticket machine**: A machine where the customer can buy, renew or scan an activated ticket.

**Renew ticket**: Buy a new identical ticket

**Scan a ticket/card**: Hold the ticket medium against the card reader in order to:

1. Show information: scan the ticket medium without changing the content (without leaving a trace)
2. Perform prearranged actions like blocking the ticket medium or downloading automatic renewal.

3. Start/continue a journey by communicating with the reader to issue or activate a ticket.
4. Register the use of the ticket without activating it (for instance new journey or transfer)

Actions covered by no. 3 and 4, were previously called validations.

**Reader**: Device on board a bus, tram, train or ferry that can scan the ticket medium.

**Reconstruction**: Recreating the content in the ticket medium to reconstruct the content as it was the last time it was used.

**Reimbursement**: Repayment of the remaining value on a ticket medium (reimbursement of tickets and/or travel money).

**Additional services**: Services that are not tied to the actual right to travel, for instance reconstruction.