

Privacy Policy Statement, date of drafting 4.2.2020

The EU General Data Protection Regulation (GDPR) 2016/679

1. Controller

TVV lippu- ja maksujärjestelmä Oy

Contact information

TVV lippu- ja maksujärjestelmä Oy
Alberga Business Park, Bertel Jungin aukio 5, 02600 Espoo
info@lmj.fi

2. Contact person in matters concerning the filing system

A data protection officer Juha Ranta
Alberga Business Park, Bertel Jungin aukio 5, 02600 Espoo
info@lmj.fi

3. Name of filing system

Customer data filing system for the Waltti travel card system

Customer data filing system for the Waltti travel card system's online and mobile services

Register for Developer account

4. Legal basis and purpose of processing personal data

Customer data filing system for the travel card system:

The data is used for managing the customer relationship between competent authority (TVV) public transport and the customer, and to implement the service. The customer's identification data is used to verify their right to buy a personal travel card and to validate the accuracy of their personal use of services.

The customer's identification number is used for the purpose of identifying the customer reliably and accurately in the filing system in order to ensure that the rights and obligations of the customer and TVV are put into effect:

- when delivering a personal travel card, which involves verifying and establishing the customer's right to buy it.
- when verifying the customer's home municipality.
 - Delivering a personal subsidised travel card requires that the customer lives in a municipality belonging to the TVV region.
 - The customer's place of domicile may have to be checked during the contractual relationship, as their home municipality may change while the card is in force. The customer is obliged to update the information on the change of home municipality on their travel card after this data has been updated in the Population Register Centre's Population Information System.
 - The discount on the payment basis varies by municipality.
 - The home municipality of a customer is checked using the Population Register Centre's Population Information System.
- when deactivating a travel card that has gone missing and establishing how many journeys remain on the card.

- when replacing a damaged travel card and establishing how many journeys remain on the card.
- when identifying the owner of a travel card which has been found.
- when identifying the customer for the purpose of refunding a ticket product on their travel card or resolving an error.
- when checking loading events and display events, if any, on the customer's travel card.
- when retrieving the data on the personal travel card and importing it into the online service application at the customer's request. The retrieval of card information requires strong digital authentication of the customer by means of online bank access codes.
- when closing down the travel card at the end of the customer relationship.
- when the customer authenticates themselves when the customer relationship is terminated.

Customer data filing system for the online and mobile services:

The data is used to produce and implement the service (products downloaded onto a travel card or a ticket identifier) and in communications relating to the management of the customer relationship. The customer's identification data is used to verify the accuracy of their use of services.

The customer's identification number is used for the purpose of identifying the customer reliably and accurately in the filing system in order to ensure that the rights and obligations of the customer, the controller and the public transport authorities are put into effect:

- when checking loading events and display events, if any, on the customer's travel card/ticket identifier.
- when retrieving the data on the personal travel card/ticket identifier and importing it into the online service application at the customer's request. The retrieval of card/ticket identifier information requires strong digital authentication of the customer by means of online bank access codes.
- when the customer authenticates themselves when the customer relationship is terminated.

Other use: The data in the customer data filing system may be used for direct marketing if the customer has given their explicit consent for this.

Personal data is processed primarily for the purpose of implementing the agreement and the legitimate interests of TVV, the controller and any third parties. Processing may also be necessary in order to comply with the statutory obligations binding the controller and/or to exercise the official authority belonging to the authorities using the filing system.

The data may also be used for planning, developing and compiling statistics of the controller's activities.

Register for Developer account:

The data is used for to purpose

- announce changes to the developer portal or data interfaces

- restrict irregularities regarding the possible interfaces and performs load balancing based on user interface keys

5. Data content of the filing system

Customer data filing system for the travel card system:

contains the following information about the public transport customers of TVV (the data does not include travel information that contains positioning data):

- Customer data
 - the start and end date of the customer relationship
 - the customer's identification data: name, the code part of their identification number, date of birth, domicile and place of residence, address, gender, mother tongue
 - for company and community customers, the company or community ID and contact information
 - phone numbers and email address, if any
 - the customer's explicit consent to direct marketing, if any
 - invoicing or repeated debit agreements, if any
 - authorisation of proxies, if any
- Basic information about the travel card
 - travel card number
 - the date the travel card was created
 - the customer's travel card-specific user group (purchase rights) and limited period of validity, if any
 - the termination date of the travel card and the code indicating the reason for termination
- The travel card's event history
 - information on actual values and monetary transactions
 - travel card's time of delivery
 - loadings made onto the travel card
 - charging of value onto the value ticket: date, time, ticket product, the amount charged and, as historical data, the balance of the travel card before and after use
 - information on the taking into use of periodic ticket products (ticket validity information)
 - event information of multi-ride and invoiced ticket products
 - the last use event (date, time and ticket product, as well as the line on which the card was used)
 - attempted uses, if any (failed validation at the card reader, reason code)
 - travel card status information (closed, open, found, defect, replaced, etc.)

Customer data filing system for the online and mobile services:

contains the following information about customers (the data does not include travel information that contains positioning data):

- Customer data
 - the start and end date of the customer relationship

- the customer's identification data: name, the code part of their identification number, date of birth, domicile and place of residence, address, gender, mother tongue and whether there is strong digital authentication of the customer by means of online bank access codes
 - for company and community customers, the company or community ID and contact information
 - phone numbers and email address, if any
 - the customer's explicit consent to direct marketing, if any
 - invoicing or repeated debit agreements, if any
 - authorisation of proxies, if any
- Basic information about the travel card/ticket identifier
 - travel card/ticket identifier number
 - the customer's travel card/ticket identifier-specific user group (purchase rights) and limited period of validity, if any
- The event history of the travel card/ticket identifier
 - information on actual values and monetary transactions
 - loadings made onto the travel card/ticket identifier
 - charging of value onto the value ticket: date, time, ticket product, the amount charged and, as historical data, the balance of the travel card/ticket identifier before and after use
 - information on the taking into use of periodic ticket products (ticket validity information)
 - event information of multi-ride and invoiced ticket products
 - the last use event (date, time and ticket product, as well as the line on which the card was used)
 - status information of the travel card/ticket identifier (closed, open, found, defect, replaced, etc.)

Register for Developer account:

contains the following information about users

- Customer data
 - first name, last name and email
 - phone number (optional)
 - username and password (no password can be seen by the registry administrator)

6. Regular sources of information

With the consent of the customer, the customer data contained in the customer data filing systems are obtained from the customer themselves, the guardian of a minor, a person authorised by the customer or the Population Register Centre's Population Information System. Personal data may be updated from the above-mentioned systems.

7. Regular data disclosure and recipient groups

Data may be disclosed to the controller, the authorities using the filing system, the product owners of the products sold in the online service and the providers of system services for the purposes described in section 4 of this Privacy Policy Statement.

Any data relating to KELA products may be disclosed to KELA.

Any data relating to school products may be disclosed to the school authorities.

8. Transfers of personal data outside the European Economic Area

No data is transferred outside the EEA.

9. Principles of filing system protection and the storage period of personal data

Customer data filing system for the travel card system and register for Developer account:

An agreement has been made between the controller and system providers on data protection. The system providers manage the storage of the customer data filing system and any data contained in it in accordance with good data processing practice and observe absolute confidentiality and secrecy.

At the end of a customer relationship, the customer's data is erased immediately, unless other legislative obligations prevent it. After the data has been erased, notifications of defects, refunds and investigating errors will no longer be possible.

Customer data filing system for the online and mobile services:

An agreement on data protection has been made between the controller, the authorities using the filing system, the product owners of the products sold in the store and system providers. The system providers manage the storage of the customer data filing system and any data contained in it in accordance with good data processing practice and observe absolute confidentiality and secrecy.

At the end of a customer relationship, the customer's data is erased immediately, unless other legislative obligations prevent it. After the data has been erased, notifications of defects, refunds and investigating errors will no longer be possible.

Access rights and access right administration

Access rights to the customer data filing systems for employees of the public transport unit and its customer service points are determined by the administrator of TVV and the persons in charge authorised by them.

Based on the assignment, the access rights of persons processing the data in the customer data filing systems (for example, at other service points, if any) are determined according to the assignment agreement between the contractor and TVV.

The processors observe an absolute duty of secrecy and confidentiality. Access rights are terminated when the person in question is transferred from the duties for which the access rights were granted to them. The obligation of secrecy and confidentiality continues even after the duties or employment relationship involving the processing of customer data ends.

The system administrator for the register for Developer account is TVV lippu- ja maksujärjestelmä Oy.

Monitoring of use and access

The use of the filing system in accordance with the user's duties, as well as attempts to access the filing system, are monitored using a file concerning the monitoring of access. The information required for monitoring is stored both in a database and a file-format log. The

subsystems of the service create the log in accordance with the control parameters. Log files are stored in a file system with restricted access rights (read-only or write access) provided only to persons in charge of maintaining the service. In general, log files are stored for a period of nine (9) months.

Particular information about the use of the filing systems is stored in the database for the purpose of access control (user ID, time stamp, search criteria and reason). The data stored in the database allows us to monitor and report on the appropriate use of the customer data filing systems. Reports needed for the monitoring of use and access are produced from this data. The file-format log is used for storing the searches and changes made in the customer information according to user and date, as well as the identifying information of the user making the search. In general, log files are stored for a period of nine (9) months.

Technical maintenance

The system providers ensure that the customer data filing system remains technically intact. Technical information concerning the system is needed for maintaining and securing the technical availability and integrity of the system. Transactions produced by the device are stored as technical data. No personal data is collected or stored as technical data.

Ensuring availability

The data is protected against intentional and unintentional destruction (by, for example, keeping the central units in locked premises protected with passage control systems and keeping backup copies of the files in a separate fire compartment), and the integrity of data is ensured by means of technical maintenance data and transaction data. The internal data communications of the system are implemented by means of closed networks. External connections have firewall protection. The system and its data communications are monitored 24/7.

10. Other rights of the data subject relating to the processing of personal data

The data subject's right to access their data (right of access)

When logging in to the **online or mobile service**, the data subject will always be able to see the majority of the information that the service contains about them.

The data subject also has the right to check what data has been stored about them in **the customer data filing system for the travel card system**. The request for checking such data must be made according to section 11 of this Privacy Policy Statement.

In principle, using the right to check the data is free. However, if the data subject's requests are manifestly unfounded or excessive, especially if made repeatedly, the controller may either charge a reasonable fee – taking into account the administrative costs resulting from supplying the data or messages or carrying out the requested action – or refuse to perform the requested action. In such cases, the controller must prove the manifestly unfounded or excessive nature of the request.

The data subject's right to demand that data be rectified or erased or that its processing be restricted

The data subject may update their own basic information in both **the customer data filing system for the travel card system and the customer data filing system for the online and mobile services**. In so far as the data subject is able to take action personally, after receiving information about an error or noticing an error themselves, they must without undue delay and on their own initiative rectify, erase or complete any incorrect, unnecessary, inadequate or outdated piece of information in the filing systems.

If the data subject is unable to correct the information themselves, they should make a rectification request in accordance with section 11 of this Privacy Policy Statement.

The data subject's right to object to the processing of their personal data

With respect to their special personal circumstances, the data subject has the right to object to the profiling and other processing activities relating to themselves, which TVV directs at the data subject's personal data in so far as the basis of processing the data is the customer relationship between TVV and the data subject. The data subject may present their objection in accordance with section 11 of this Privacy Policy Statement. In connection with their objection, the data subject must specify the particular situation, based on which they object to the processing of their data. TVV may refuse to carry out the request relating to the objection on grounds provided by law.

The data subject's right to transfer data from one system to another

In so far as the data subject has themselves supplied information processed on the basis of the data subject's consent to **the customer data filing system for the travel card system and the customer data filing system for the online and mobile services**, the data subject has the right to obtain such information for themselves, usually in a machine-readable form, and the right to transfer such data to another controller.

The data subject's right to lodge a complaint to the supervisory authority

The data subject has the right to lodge a complaint to the competent supervisory authority if the controller has failed to comply with the applicable data protection regulations in their activities.

Other rights

If the data subject's personal data is being processed on the basis of their consent, the data subject has the right to withdraw their consent by informing TVV of their withdrawal in accordance with section 11 of this Privacy Policy Statement.

11. Contact details

In all questions relating to the processing of personal data and situations relating to the use of a data subject's rights, the data subject should contact the service point of TVV or write to: XX, Address:

TVV lippu- ja maksujärjestelmä Oy
Alberga Business Park, Bertel Jungin aukio 5, 02600 Espoo
info@lmj.fi

TVV may ask the person making the request to prove their identity. The controller will reply to the customer within the time limit set in the EU General Data Protection Regulation (usually within one month).