

# Requirements for accepting internet card payments

Valid from 13.01.2018

## Contents

<b>General requirements for the point of sale website</b>	<b>1</b>
<b>Requirements for the transaction notice</b>	<b>2</b>
<b>Fraud prevention</b>	<b>2</b>
<b>Annulment of a transaction</b>	<b>2</b>
<b>Recurring payment and payment with saved card data</b>	<b>3</b>
Information presented at the point of sale	3
Execution of transactions	3
Termination	3

## General requirements for the point of sale website

1. When requesting client data, the merchant shall use a secure connection, the certificate of which has been provided by a trusted certificate authority.
2. Card data is transferred via the server of the service provider of the payment solution to ensure that the connection between the cardholder and the processor is always secure.
3. The merchant can access the transaction report, but not the full card number.
4. Before executing the transaction, the merchant shall make visible to the cardholder the following information at the point of sale:
  - privacy policy and information on data security, i.e. information on:
    - whether the personal data, which the cardholder has presented to the merchant, will be used or not and if yes, then for what purpose;
    - the fact that the merchant will not see the entered card data.
  - merchant's full name;
  - merchant's registry code;
  - merchant's country of location and postal address;
  - full list of ordered goods or services together with prices;
  - an accurate description of the product or service, providing the cardholder with a sufficient overview of what is being offered. Special attention in the description is paid to whether these goods or services are legal and can be used outside the merchant's country of location (for example, a merchant offering electrical equipment must present the conditions for effective supply voltage, which is different in each part of the world);
  - logos (Visa/MasterCard) and commercial labels (MasterCard SecureCode, Verified by Visa) of accepted cards. All logos and commercial labels have been presented with the same proportions and no brand is preferred over the others. The merchant will obtain correct logos from the service provider of the payment solution or the bank;
  - transaction currency and cross-exchange rates for the best known currencies (depending on the target market) together with reference to their source and frequency of updating;
  - the procedure for delivering or sending the goods, postal charges to be added, the procedure for determining these and notifying the cardholder thereof and restrictions on shipping the goods (e.g. goods are not shipped outside Estonia, goods with large dimensions are sent only via a specific service, shipping is possible only to certain countries, etc.);

- the final cost of transaction with the postal charge and a reference to possible additional costs (such as cardholder's obligation to pay customs duty and VAT);
  - notification about the cardholder's right of withdrawal: the procedure for returning the goods, time limits, warranty terms and the procedure for the exchange of goods;
  - information on how the cardholder will receive the transaction confirmation and how the merchant will inform of possible complications when handling the goods;
  - customer service telephone number and e-mail address, and the procedure for giving feedback: in the case of a phone number, operating hours according to local time must be added with an indication of the time zone (GMT+2); in the case of an e-mail, the estimated response time to inquiries must be added; the communication languages of channels are visible.
5. The merchant shall follow the legislation of the country of destination, the European Union and the OECD applicable to e-commerce and distance selling to a cardholder.
  6. The merchant is able to prove in a format which can be reproduced that the cardholder has, before confirming the transaction, agreed to the conditions of sale of the service or goods.
  7. The merchant is responsible for the accuracy of the information and offers made at the point of sale. In the case of significant changes in the offered goods, service or assortment, the merchant shall inform the bank thereof in advance.

## Requirements for the transaction notice

8. After the merchant has received a positive response to the transaction from the bank, the merchant shall display the transaction notice to the cardholder. This shall be presented in a format, which is easy to print or save.
9. If the e-mail address is known, the merchant shall send the transaction notice to the cardholder also via e-mail.
10. The transaction notice displayed to the cardholder shall show:
  - information required by legislation;
  - information that the transaction has been paid for by card;
  - a unique identification number of the transaction, which helps both the cardholder and the merchant keep account of the transactions and solve possible problems;
  - internet address of the point of sale.
  - recommendation to print or save the transaction notice and keep it.

## Fraud prevention

11. The merchant is responsible for all transactions made at its point of sale.
12. The merchant shall provide training to its employees in accordance with these instructions and inform them of risks involved in accepting card payments.
13. The merchant shall use organisational, physical and IT security measures to protect against unauthorised use of the certificates, keys, usernames and passwords or other means that are required to use the payment solution. The merchant shall inform the bank immediately if there is a risk that an unauthorised person has gained access to the said means.
14. Before dispatching the goods or providing the service, the merchant shall check the data of the transaction.
15. In the case of a suspicious transaction, the merchant shall compare its data to any previously committed fraud.
16. The merchant shall pay particular attention to transactions, where:
  - goods are sent or services are ordered to the same address by several cardholders or several cards are used for ordering;
  - the purchase sum is larger than usual;
  - transactions have been made from the same IP address with different cards or goods or services have been ordered to different recipients.
17. Upon detecting a suspicious transaction, the merchant shall immediately contact the bank.
18. If the merchant has detected a suspicious transaction, the bank may suspend the processing of a transaction for the duration of an investigation or to annul a transaction. In this case, the bank will notify the merchant of inspecting the transaction and the merchant shall not ship the goods.

## Annulment of a transaction

19. To annul a transaction, the merchant shall send a request to the bank alongside the data of the transaction or commence the cancellation of the transaction from the portal of the service provider of the payment solution. The

merchant is not allowed cancel the transaction in any other manner and return the money to the cardholder. The merchant shall indicate also the reason for the cancellation in the request.

20. After the annulment of the transaction, the merchant shall notify the cardholder of the annulment, who has returned the goods and is requesting the returning of the sum of the transaction.

## Recurring payment and payment with saved card data

### Information presented at the point of sale

21. If the merchant enables for the cardholder recurring payments or payments with saved card data, the merchant shall conclude an agreement with the cardholder for using such a service. In the agreement, the cardholder shall be given all information about the rights and obligations of the cardholder and the merchant.  
Among other things, the merchant shall present the following information in the terms and conditions of the agreement:
  - what kind of data is saved (card number in a hidden manner, showing only the last 4 digits) and how the data is used;
  - how the merchant will inform the cardholder of changes in the agreement. The merchant shall be responsible for ensuring that the amendment of the agreement is in conformity with the legislation. When making changes, the cardholder must be informed of the right to withdraw from the service;
  - how the cardholder can withdraw from the service.
22. In addition, before making the first recurring payment, the merchant shall obtain the cardholder's consent, which shall include the following information:
  - whether the transaction sum is fixed or variable. In the case of a fixed amount, the agreement must also state the transaction amount and the currency. In the case of a variable amount, the logic of how the transaction amount is formalised shall be indicated.
  - whether the transaction date is fixed or variable. In the case of a fixed date, the respective date/interval shall be provided. In the case of a variable date, an event or another condition shall be given, on which the transaction date depends.
23. The conditions of the agreement/consent specified in clause 21 and 22 must be presented to the cardholder clearly and separately from other conditions applicable at the merchant and the cardholder shall confirm the acceptance of the terms and conditions in a clear manner (such as by ticking an appropriate box or by clicking on "I agree").
24. The merchant shall save the cardholder's agreement/consent in a format which can be reproduced for the recurring payments or for the payments with saved card data during the validity of the service and within two years after the last recurring payment / payment with saved card data and if necessary, shall present it to the bank within two settlement days.
25. The merchant shall show to the cardholder in their profile view at the point of sale the cardholder's cards, which are used for making recurring payments or payments with saved card data. The merchant shall also show the hidden card number with only the last four digits visible.
26. The merchant shall apply relevant and sufficient measures to ensure that a payment with saved card data can be made only by the cardholder.
27. Withdrawal from the recurring payment or payment with saved card data must be easy for the cardholder. After the receipt of a notice of withdrawal, the merchant will stop making recurring payments and end the processing of saved client data.

### Execution of transactions

28. All transactions must be authorised.
29. Upon concluding an agreement for making recurring payments or saving card data, strong authentication measures of the cardholder shall be applied.
30. If a non-permissive response code is received upon the authorisation of a transaction when making a recurring payment, the merchant may try to authorise the transaction again up to four times within the next 16 days, until an acceptable response code is received.

### Termination

31. The bank may restrict or terminate the acceptance of recurring payments or payments with saved card data by informing the merchant one month in advance thereof. If the merchant violates contractual obligations, the bank may restrict or terminate the acceptance of such payments without an advance notice.