



Merchant Agreement for MasterCard, Maestro,
Visa, Visa Electron, V PAY, JCB, China UnionPay
and American Express

Business Procedures



Table of Contents

1. Introduction	2
2. Face-to-Face Transactions	2
2.1. Checking of Cards, Measures to Reduce Fraud, etc.	2
2.2. Requirements to Terminals	2
2.3. Requirements to the Installation of PIN Terminals	3
2.4. Completion of Transactions	3
2.4.1. PIN Transactions	3
2.4.2. Signature-based Transactions.....	3
2.4.3. Cardholder Receipt.....	4
2.5. Depositing of Transactions with Teller	4
2.6. Backup	4
2.7. Security Requirements	5
3. Non-face-to-face Transactions – Self-service Terminals	5
3.1. Requirements to your Equipment	5
3.2. Cardholder Receipt.....	5
3.3. Depositing of Transactions with Teller	5
3.4. Security Requirements.....	6
4. Non-face-to-face Transactions – e-commerce, MOTO, recurring payments	6
4.1. Requirements to your Web Site.....	7
4.2. Checks; Measures to Reduce Fraud etc.....	7
4.3. What is an authorisation and what should you do?	7
4.4. E-commerce Payments	7
4.4.1. Procedure.....	8
4.4.2. Acceptance of the Payment Transaction	8
4.4.3. Order Confirmation/Cardholder Receipt	8
4.4.4. Depositing of Transactions.....	8
4.4.5. Security Requirements	9
4.5. Mail and Phone Order	9
4.5.1. Requirements to Mail Order Forms	9
4.5.2. Requirements in connection with Phone Orders, incl. Order Confirmation.....	9
4.5.3. Procedure.....	10
4.5.4. Mail and Phone Order Cardholder Receipt.....	10
4.5.5. Depositing of Transactions.....	10
4.5.6. Security Requirements	10
4.6. Subscriptions (Recurring Payments)	10
4.6.1. Requirements for Recurring Payments.....	10
4.6.2. Security Requirements	11

1. Introduction

This document is part of the Merchant Agreement. The Business Procedures regulate the issues referred to in the General Rules. The definitions used in the General Rules are also applicable to the Business Procedures.

Which Card Types may be used

Each chapter contains a table illustrating which card types may be used for the different transaction types.

2. Face-to-Face Transactions

Card type	Transaction type							
	Chip/PIN		Magnetic stripe/PIN		Chip/signature		Magnetic stripe/signature	
	Online	Offline	Online	Offline	Online	Offline	Online	Offline
MasterCard	+	+	+	-	+	+	+	-
Maestro	+	+	+	-	+	-	+	-
Visa	+	+	+	-	+	+	+	-
Visa Electron	+	+	+	-	+	-	+	-
V PAY	+	+	-	-	-	-	-	-
JCB*	+	+	+	-	-	-	+	+
China UnionPay*	-	-	+	-	-	-	+	-
American Express**	-	-	+	-	-	-	+	-

*) The PIN of the JCB and China UnionPay can only be used in terminals, which are able to process PINs of more than 4 digits. MasterCard- and Visa card products may also have PINs of more than 4 digits

**) American Express cards may have a chip but not all terminal types are approved for the reading of American Express chip! Foreign-issued American Express cards may typically only be used with a signature

2.1. Checking of Cards, Measures to Reduce Fraud, etc.

When signature-based transactions are to be conducted and you are not certain that the card is genuine or that it is the genuine cardholder using the card; you must check the card.

Further information is available in the leaflet "Security in connection with card payments" which also provides you with useful advice how to spot attempts at fraud and what to do.

2.2. Requirements to Terminals

Face-to-face transactions as defined in the General Rules require a terminal that is able to read the card's chip/magnetic stripe and provides the cardholder with the possibility of entering his/her PIN or signing a cardholder receipt.

The merchant may solely install terminals that are approved by Teller, cf. www.pbs.dk for further information on approved terminals. Installation of terminals that are not chip-enabled

is not permitted. Additionally, newly installed and replaced terminals must, besides the EMV-chip reading device, have a PIN pad.

For face-to-face transactions, it is NOT allowed to enter the card number and other card data in a payment solution, except where this is specifically approved by Teller, e.g. in a backup situation, see section 2.6, or where permitted in the Additional Rules for Hotels and Car Rental.

If your terminal is chip-enabled, and the card carries a chip, the chip must always be read. If the chip is unreadable, you may attempt to complete the transaction using the magnetic stripe, if the card allows fall-back to magnetic stripe, cf. the table. Be aware that certain cards will be rejected. Be also aware that certain terminals are unable to read the American Express chip. Follow the instructions on the terminal display.

See the manual for the terminal for further instructions.

2.3. Requirements to the Installation of PIN Terminals

In order to provide the cardholder with the possibility of protecting the PIN from being disclosed to any third party when entered, the following measures must be taken when installing PIN terminals:

The placing of the PIN Entry Device:

- The placing of the PIN Entry Device must allow the cardholder to position himself/herself close to the PIN Entry Device
- It must be possible for the cardholder – without inconvenience – to cover the entry of the PIN-code with hands or body

Surroundings:

- The placing of the PIN Entry Device must not allow the disclosure of the PIN-code to any third parties by means of mirrors, video cameras or the like in the surroundings

The terminal may not be modified, and it is not allowed to remove the privacy shield. In case of tampering or attempts at tampering with the terminal, you must contact Teller immediately.

2.4. Completion of Transactions

The following instructions must be observed when conducting card transactions:

2.4.1. PIN Transactions

Transactions must always be online authorised, unless otherwise specifically agreed with Teller or in connection with backup, cf. section 2.6.

- You must enter the total transaction amount into the terminal
- You may not round off the transaction amount (stipulated by Danish law)
- If your terminal is DCC-enabled, i.e. you are able to offer the cardholder to pay in his/her billing currency, you must ask the cardholder to choose currency prior to completing the transaction
- In the case of PIN transactions, authorisation is requested upon the cardholder's approval of the amount
- You must always check that the terminal and cardholder receipt show an "approved" message

- If you are not sure that the genuine cardholder is using the card, you must check the card and ask the cardholder to provide further identification. Check whether a photo, if any, on the card looks like the cardholder
- If you are still not sure that the genuine cardholder is using the card, you must cancel the transaction in the terminal and possibly ask the customer to pay by other means
- If authorisation is declined, the transaction cannot be completed. Observe the instructions on the terminal display
- If the terminal shows a code meaning that you should confiscate the card, you must decline to accept the card as means of payment and, if possible, you should confiscate the card. Confiscated cards must be sent to Teller

If the cardholder does not have a PIN, you may complete a signature-based transaction, cf. below, if the card allows signature-based transactions, cf. the table. Follow the instructions on the terminal display.

2.4.2. Signature-based Transactions

Transactions must always be online authorised unless otherwise specifically agreed with Teller or in connection with backup, cf. section 2.6.

- In connection with signature-based transactions, you must always check the card, see section 2.1 and the document "Security in connection with card payments", if applicable
- You must enter the total transaction amount into the terminal
- You may not round off the transaction amount (stipulated by Danish law)
- If your terminal is DCC-enabled, i.e. you are able to offer the cardholder to pay in his/her billing currency, you must ask the cardholder to choose currency prior to completing the transaction
- You must check that the date and amount stated on the cardholder receipt are correct and that the non-truncated digits of the card number appearing on the cardholder receipt are identical with the card number that is embossed or printed on the card, if applicable
- When the cardholder has signed the cardholder receipt you must check that the signatures on the cardholder receipt and the card are matching
- If you are not sure that the genuine cardholder is using the card, you should request additional identification
- If you are still not sure that the genuine cardholder is using the card, you must cancel the transaction in the

terminal, destroy the sales slip and possibly ask the customer to pay by other means

- If authorisation is declined, you may not complete the transaction. Observe the instructions on the terminal display
- If the terminal shows a code meaning that you should confiscate the card, you must decline to accept the card as means of payment and, if possible, you should confiscate the card. Confiscated cards must be sent to Teller

2.4.3. Cardholder Receipt

The cardholder is entitled to a cardholder receipt for any transaction. You must hand out the cardholder receipt to the cardholder. If in the case of errors, your terminal is unable to print a cardholder receipt, you must submit a cardholder receipt, if so requested by the cardholder.

2.5. Depositing of Transactions with Teller

Transactions are deposited with Teller electronically from the terminal or as otherwise agreed. Transaction data must be deposited as soon as possible and must be received by Teller no later than the third calendar day after the transaction date, cf. also the General Rules. The procedure appears from the terminal vendor's manual for the terminal. Transactions are registered by Teller on the first banking day after the transactions are deposited.

2.6. Backup

You may use the terminal's offline or key entry function to complete the transaction. The table shows which cards may be used for offline transactions. Refer to the terminal vendor's manual for the terminal for further information.

If your terminal is out of order, you may use a paper slip, possibly in combination with an imprinter (zipzap machine), or another procedure specifically agreed with Teller.

You must observe the following procedure in the backup situation:

- In connection with signature-based transactions, you must always check the card, see section 2.1 and the document "Security in connection with card payments". If the card is not valid or is expired, you may not complete the transaction.
- Call Teller on telephone 44 89 21 80 in order to obtain an authorisation code for the total transaction amount

- You must enter the total transaction amount into the terminal as usual
- You may not round off the transaction amount (stipulated by Danish law)
- The authorisation code must be entered into the terminal
- Have the cardholder sign the cardholder receipt and check that the signatures on the cardholder receipt and the card are matching
- Hand out the card and the cardholder receipt to the cardholder
- If you are not sure that the genuine cardholder is using the card, you should request additional identification
- If you are still not sure that the genuine cardholder is using the card, you must cancel the transaction and ask the customer to pay by other means
- If authorisation is declined, you may not complete the transaction
- If you are asked to confiscate the card, you must decline to accept the card as means of payment and, if possible, you should confiscate the card. Confiscated cards must be sent to Teller
- If you are using paper slips, and it is not possible to make an imprint of the card or the card imprint is not legible, you must fill out the paper slip/cardholder receipt by hand with all data that appear from the front of the card. Follow the instructions above. Remember to include the authorisation code in the sales slip/cardholder receipt. Furthermore, you must ask the cardholder for further identification

Paper slips must be submitted to Teller – indicate "backup procedure" on the summary card. If there are no errors or shortcomings in the data, the transactions will normally be registered by Teller on the first banking day after the paper slips were sent.

Be aware that a maximum transaction amount for offline transactions may be defined for your terminal.

Be aware that certain card types cannot be used for offline transactions. Some cards do not carry an embossed card number and consequently they cannot be used to complete transactions using sales slips; i.e. such card must be read by a terminal.

2.7. Security Requirements

Refer to the chapter on security requirements in the General Rules. Check the section at www.pbs.dk concerning PCI DSS to learn more about the procedure you should follow in order to document your observance of the security requirements.

3. Non-face-to-face Transactions – CAT/UAT

Card type	Transaction type							
	Chip/PIN		Magnetic stripe/PIN		Chip/no PIN		Magnetic stripe/no PIN	
	Online	Offline	Online	Offline	Online	Offline	Online	Offline
MasterCard	+	+	+	-	+	+	+	-
Maestro	+	+	+	-	-	-	-	-
Visa	+	+	+	-	+	+	+	+
Visa Electron	+	+	+	-	+	+	+	-
V PAY	+	+	-	-	-	-	-	-
JCB**	+	+	+	-	-	-	+	+
China UnionPay**	-	-	+	-	-	-	-	-
American Express***	-	-	+	-	-	-	+	+

*) Visa requires that self-service terminals are chip-enabled and have a PIN-pad. In specific cases, a waiver from the PIN requirement may be obtained; see www.pbs.dk

**) The PIN of the JCB and China UnionPay can only be used in terminals, which are able to process PINs of more than 4 digits. MasterCard- and Visa card products may also have PINs of more than 4 digits

***) Foreign American Express cards may be declined by PIN terminals, since PIN check is not supported by the terminals

3.1. Requirements to your Equipment

You may only install CAT/UAT that have an EMV chip reading device and a PIN pad, unless otherwise specifically agreed with Teller.

Your procedures for the acceptance of cards must be approved by Teller and possibly the international card organisations before the payment solution is brought into use. The user manual of the terminal must be approved by Teller.

For CAT/UAT that do not have a PIN-pad, an amount maximum per transaction has been defined. The amount maximum will appear from your merchant agreement.

CAT/UAT may solely be used for the sale of services and may not dispense cash or issue scrips that may be exchanged for cash.

3.2. Cardholder Receipt

The CAT/UAT must have a function offering the cardholder to print out a receipt. If the cardholder requests a cardholder receipt, this must be printed out.

If in the case of errors, the terminal is unable to print a cardholder receipt, this must be shown to the cardholder. You must be able to submit or hand out a cardholder receipt, if so requested by the cardholder.

3.3. Depositing of Transactions with Teller

Transactions are deposited with Teller electronically from the terminal or as otherwise agreed as soon as possible. Transaction data must be deposited as soon as possible and must be received by Teller no later than the third calendar day after the transaction date, cf. also the General Rules. The procedure appears from the terminal vendor's manual for the terminal. Transactions are registered by

Teller on the first banking day after the transactions are deposited.

3.4. Security Requirements

Refer to the chapter on security requirements in the General Rules. Check the section at www.pbs.dk concerning PCI DSS to learn more about the procedure you should follow in order to document your observance of the security requirements.

Besides the security requirements stipulated in the PCI DSS, the below mentioned requirements are applicable to CAT/UAT:

- Only staff educated for the purpose may be granted access to card readers and PIN entry devices
- Access to the following must be particularly restricted:
 - Access to the card reader and PIN entry device of the terminal
 - Mandates to put the programmes/systems into operation
- Codes/keys to the terminal must be stored in a safe manner and may only be handed out to authorised staff
- The terminal cabinet must always be locked, also when the terminal is not in use. The terminal must not be able to function when the cabinet is open
- You may not modify the physical functions of the terminal, e.g. remove the PIN privacy shield. The placing of the PIN Entry Device must not allow the disclosure of the PIN to any third parties by means of mirrors, video cameras or the like in the surroundings
- You may only use approved self-service terminals in connection with card payments. You must currently monitor alarms from the terminals and secure the terminals adequately to prevent unauthorised access or attempt at break-in or the like. You must have procedures for the handling of unexpected or unusual incidents
- In case of tampering or attempts at tampering with the terminal, you must immediately contact Teller, cf. the telephone list
- You must have reconciliation procedures, which ensure that the correct number of transactions is deposited with Teller. Furthermore, backup procedures must be established to ensure correct re-transmission/re-delivery of transaction data 5 banking days after the transactions were deposited with Teller

4. Non-face-to-face Transactions – e-commerce, MOTO, recurring payments

Card type	Transactions type			
	with authentication **	without authentication	Mail order /phone order	Recurring payments
MasterCard	+	+	+	+
Maestro	+	-	-	-
Visa	+	+	+	+
Visa Electron *	+	+	-	-
V PAY	-	-	-	-
JCB	+	+	+	+
China UnionPay	-	-	-	-
American Express	-	+	+	+

*) If e-commerce transactions are permitted by the card issuer

***) MasterCard SecureCode, Verified by Visa and J-Secure

4.1. Requirements to your Web Site

The following information must, as a minimum, be displayed clearly on your web site:

- Your name (name of your business), company registration number, and address; incl. the country where you have your business domicile
- The telephone number and e-mail address of your customer service/contact person
- A complete description of the products or services for sale (incl. prices, taxes, duties, any other fees)
- Delivery policy and shipping costs and the rules for the cardholder's right of cancellation, incl. whether or not the cardholder must pay the costs in connection with returning the products or services
- That cardholders can pay by payment card
- The trademarks of the cards that you accept. The trademarks must appear where all payment options are offered
- Transaction currency (e.g. DKK)
- Export restrictions, if any

Furthermore, your web site must contain a function where the cardholder may enter his/her CVC/CVV.

For further information, please refer to applicable law, including consumer law, marketing practices law etc.

Your web site may not provide the cardholder with the possibility of entering his/her PIN. Your web site may not provide the cardholder with the possibility of entering card data unencrypted. Besides, you may not provide the cardholder with the possibility of transmitting orders containing card data via e-mail, unless in encrypted form. The encryption method must be approved by Teller.

4.2. Checks; Measures to Reduce Fraud etc.

In the case of non-face-to-face transactions, the merchant and the cardholder do not meet for which reason it is not possible to check the card that is used or who is using it.

However, you can take certain measures that may help reduce the risk of fraud in your business. Read more in the document "Security in connection with card payments".

4.3. What is an authorisation and what should you do?

An approval response to an authorisation request means that the card is valid and that the amount of the authorisa-

tion request has been reserved at the cardholder account. In order to avoid problems for the cardholder, if you are for example not able to deliver the goods/render the service, it is important that you make sure not to authorise – and thereby reserve – the same transaction amount several times.

If you are not able to deliver the goods or render the service ordered by the cardholder within a few days after the order was placed, or if you are not sure that you are able to deliver, you may not send an authorisation request to Teller for the total amount of the order. You may forward an authorisation request for DKK 1 (or one unit of your local currency) in order to ensure that the card is not blocked. Subsequently, you may authorise when you are ready to deliver the goods or render the service.

You may divide the delivery into partial deliveries. This means that you should forward an authorisation request for the actual amount of each partial delivery.

The same applies, if you use MasterCard SecureCode, Verified by Visa and J/Secure. You must store the response to the authentication request until you are ready to forward the authorisation request. The authentication response must be included in the authorisation response to Teller. Be aware that the authentication response may only be used once.

CVC/CVV must always be included in the authorisation requests for all card payments. In case of subscriptions or other types of recurring or split payments, the CVC/CVV must be included in the original transaction data (the first transaction). If the CVC/CVV is not included or is not correct, authorisation may be declined.

Teller's systems and our requirements for payment gateways support the above mentioned functions. Therefore, you must ensure that the payment gateway you are using handle your requests, responses and transactions correctly.

4.4. E-commerce Payments

You may avail yourself of MasterCard SecureCode, Verified by Visa, J/Secure and/or CVC/CVV.

If you avail yourself of MasterCard SecureCode, Verified by Visa, J/Secure, the relevant trademarks must be shown together with the trademarks for the cards. For further information, refer to www.pbs.dk

4.4.1. Procedure

The following procedure is used in connection with an e-commerce payment transaction:

- The cardholder enters his/her order and the data necessary to complete the payment transaction:
 - Card number
 - Expiration date
 - CVC/CVV

If you avail yourself of MasterCard SecureCode, Verified by Visa, J/Secure:

- Authentication of the cardholder will automatically be requested by Teller, when the request is received.
- You will receive one of the following responses to your authentication request:
 - (1) Authentication OK – this means that authorisation can be requested
 - (2) The cardholder could not be authenticated (e.g. the cardholder does not participate) – this means that authorisation can be requested
 - (3) Authentication declined (code incorrect, communication error or the like) – this means that you may request authorisation. Completion of the transaction is, however, at your own risk
 - (4) Cardholder entered incorrect code and exceeded the maximum number of attempts – this means that you may not request authorisation – decline acceptance of card!
- The response you receive also contains an authorisation response; either approved or declined.
- If authorisation is declined, you may under no circumstances complete the transaction

If you do not avail yourself of MasterCard SecureCode, Verified by Visa, J/Secure:

- An authorisation request is transmitted to Teller and you will receive an authorisation response; either approved or declined
- If authorisation is declined, you may under no circumstances complete the transaction

Encryption must be applied when card data is entered.

CVC/CVV must never be stored. Thus, you must delete

CVC/CVV which you have received together with the cardholder's order as soon as the card payment has been authorised.

4.4.2. Acceptance of the Payment Transaction

Before the cardholder accepts the payment transaction in connection with his/her purchase, the following information must as a minimum appear from the screen:

- A unique description of and price for the individual products or services ordered by the cardholder
- The total amount to be paid by the cardholder (including a specification of any taxes, duties, shipping costs and any other charges)
- You are not permitted to round off the amount (stipulated by Danish law)
- Transaction currency (e.g. DKK)
- That payment is made by payment card
- Expected delivery date
- Terms of delivery, and rules on the cardholder's right of cancellation/return, including whether the cardholder is to pay the costs of returning the product or service
- Name of the recipient of the product or service
- Delivery address

For security reasons, the delivery address should not be a P.O. Box.

4.4.3. Order Confirmation/Cardholder Receipt

The electronic cardholder receipt must as a minimum contain the following data:

- Your name (name of your business)
- Your e-mail address
- A description of the products or services ordered
- Order number/transaction number
- Transaction date
- Transaction amount
- Transaction currency (e.g. DKK)
- Transaction type (debit/credit)
- Delivery date
- That the payment transaction has been completed (if cardholder receipt)

4.4.4. Depositing of Transactions

Transaction data must be deposited electronically with Teller as soon as possible, however, transactions may not be deposited until goods are delivered/services rendered

(transaction date). Transactions must be received by Teller not later than 3 calendar days after the transaction date. Transactions are normally registered by Teller on the first banking day after depositing.

4.4.5. Security Requirements

Refer to the chapter on security requirements in the General Rules. Check the section at www.pbs.dk concerning PCI DSS to learn more about the procedure you should follow in order to document your observance of the security requirements.

4.5. Mail and Phone Order

When you sell goods via mail and telephone order, you must avail yourself of a payment solution that is approved by Teller for the depositing of your payment transactions.

4.5.1. Requirements to Mail Order Forms

An order form to be used for mail orders must contain the following fields (besides the name, address, etc. of your business), which the cardholder must fill out in connection with his/her order:

- Cardholder's name
- Cardholder's address
- Cardholder's telephone number
- Card type
- Card number
- Date of expiry/issue of the card
- CVC/CVV of the card
- Number and type of each product/service ordered
- The amount for each product/service
- Transaction currency (e.g. DKK)
- Shipping costs, if any
- Total amount
- Recipient of the product/service (if not the cardholder)
- Delivery address (if not the cardholder's address)
- Date
- Signature

CVC/CVV may never be stored, therefore you must delete/destroy the CVC/CVV when the payment transaction has been authorised. Read more about authorisation in section 4.3.

Furthermore, the rules for the cardholder's right of cancellation must be included in the order form.

Teller must approve the order form before it is brought into use.

Order forms containing card data may not be forwarded by the cardholder via e-mail or other networks, unless they are encrypted. Furthermore, the order form may not be forwarded as an "open postcard" which would enable the disclosure of card data. Thus, the order form must always be forwarded in an envelope.

4.5.2. Requirements in connection with Phone Orders, incl. Order Confirmation

When the cardholder is placing his/her order by phone order, you must provide the cardholder with adequate information about the terms and conditions applicable to the purchase, including shipping costs and other costs.

You must as a minimum request the following information from the cardholder in order to complete the payment transaction:

- Card type
- Card number
- Date of expiry/issue of the card
- CVC/CVV of the card

CVC/CVV may never be stored, therefore you must delete/destroy the CVC/CVV when the payment transaction has been authorised. Read more about authorisation in section 4.3.

If the product/service cannot be delivered/rendered immediately, you must at once forward an order confirmation to the cardholder. The order confirmation must be sent to the cardholder's address and must contain the following information:

- That payment is made by card
- Card type
- Amount
- Transaction currency (e.g. DKK)
- Shipping costs, if any
- If the product/service is to be delivered/provided to an address different from the cardholder's address, you must send the order confirmation to the cardholder's address
- If the amount cannot be determined in advance and thus does not appear from the order confirmation, you must

be able to provide proof that the cardholder specifically has consented to the completion of the transaction

4.5.3. Procedure

When a cardholder has placed an order by mail or phone order, you must observe the below mentioned procedure:

- You must request authorisation electronically via your terminal or payment solution, by telephone (+45 44 89 21 80), or as specifically agreed with Teller, cf. your merchant agreement
- If the card is blocked or authorisation is declined, Teller will notify you accordingly and the payment transaction must not be completed
- If CVC/CVV is not included or is not correct, the transaction may be rejected

4.5.4. Mail and Phone Order Cardholder Receipt

You must send an invoice/cardholder receipt to the cardholder not later than at the date when the transaction is deposited with Teller. The invoice/cardholder receipt must as a minimum contain the following data:

- The date of shipment of the products/services ordered
- Transaction amount
- Transaction currency (e.g. DKK)
- Card type
- Card number (truncated)

4.5.5. Depositing of Transactions

Transaction data must be deposited electronically with Teller as soon as possible, however, transactions may not be deposited until goods are delivered/services rendered (transaction date). Transactions must be received by Teller not later than 3 calendar days after the transaction date. Transactions are normally registered by Teller on the first banking day after depositing.

4.5.6. Security Requirements

Refer to the chapter on security requirements in the General Rules. Check the section at www.pbs.dk concerning PCI DSS to learn more about the procedure you should follow in order to document your observance of the security requirements.

4.6. Subscriptions (Recurring Payments)

If you wish to be able to complete recurring payments with cards, you must contact Teller in order to be approved for

this function. You must submit a copy of your terms and conditions to Teller prior to commencing the recurring payments.

4.6.1. Requirements for Recurring Payments

The below mentioned requirements are applicable to recurring payments.

You must enter into an agreement with the cardholder allowing you to complete payment transactions by means of the card data provided by the cardholder. The agreement must include:

- Card number
- Card expiration date
- CVC/CVV of the card
- Information about the criteria for the completion of recurring transactions by means of the card number
- Information about the procedure for the provision of a cardholder receipt
- Information about the cardholder's responsibilities and liability
- Information about the procedure for renewal and deletion of card number
- The cardholder's acceptance of terms and conditions, including:
 - The cardholder's acceptance of criteria for the completion of transactions by means of the card number
 - The acceptance of prices

CVC/CVV may never be stored, therefore you must delete/destroy the CVC/CVV when the payment transaction has been authorised. Read more about authorisation in section 4.3.

Registration for recurring payments enables you to conduct subsequent transactions as agreed with the cardholder without having to submit the CVC/CVV in the authorisation request.

The cardholder must either sign the agreement or accept the agreement directly on your web site followed by your written confirmation to the cardholder. Terms, conditions and prices must be accessible to the cardholder when entering into the agreement.

You must establish adequate procedures for the registration, renewal and deletion of card data.

Your procedure for the deletion of card data must provide for data to be deleted from your customer database immediately upon the cardholder's request.

If you discontinue offering recurring payments, you must notify Teller thereof.

You must avail yourself of a payment solution that is approved by Teller for the depositing of your card payments.

4.6.2. Security Requirements

Refer to the chapter on security requirements in the General Rules. Check the section at www.pbs.dk concerning PCI DSS to learn more about the procedure you should follow in order to document your observance of the security requirements.

