Payment Services

# Secure processing of card payments in the hotel business

## Guidelines from SIX Payment Services

## Contents

# Preface

**Dear customer,**

More and more people appreciate the flexibility and the independence of paying with credit and debit cards. And more and more acceptance partners, like yourself, are pleased with the growing card revenue.

It is important to heed several security precautions so that your business is not adversely affected. This is because the success of cashless payment, has unfortunately, also brought scam artists into action – particularly in the hotel business. Several hotels in Switzerland have, in recent years, become victims of card data theft. Hazards often lie in wait in places we would never expect them.

As a leading company in "acquiring" and "processing", SIX Payment Services is committed to supporting you around the issue of "card data security" by any means possible. That is why we have put together these guidelines.

The suggestions and tips compiled in this handbook enable smooth and customer-friendly processing of card transactions – from reservation, to booking, to check-out.

One section addresses the topic of data protection and the so-called "Payment Card Industry Data Security Standard" (PCI DSS for short) that was defined by the leading card organisations – particularly Visa and MasterCard – to handle sensitive data. The PCI DSS applies worldwide, and is intended for all parties that transfer, process or save card data.

Direct your attention to this set of guidelines and gain an overview of what could be implemented or optimized in your hotel business. Your guests will be satisfied even after paying their bill, and their holiday experience will remain unforgettable.

Do you have any questions about the topics addressed in this handbook? The PCI team at SIX Payment Services will be happy to help you. All you need to do is write an e-mail to hotelbestpractice@six-group.com.

We wish you continued success in your business!

Your SIX Payment Services PCI team

# Hotel reservation guarantee per credit card

## How to properly proceed

Holders of a Visa, MasterCard, Diners Club, Discover, UnionPay or JCB can guarantee the first overnight stay in a hotel using their card. As a hotel and/or booking agent, it is essential that you observe a number of important points listed in this leaflet. Make sure that the booking agent forwards all information regarding the reservation/cancellation to you immediately.

### How to make a reservation

1. You should ask your guest for the following information when making the reservation:

**1** Credit card number and expiration date

**2** Last name and first name of the cardholder (must be the same as the guest), address, phone/fax number and e-mail address of the cardholder

**PCI DSS guidelines**
Observe the guidelines of the security standard defined by the leading card organisations: PCI DSS. You will find explanations on page 10 of this handbook.

2. You should inform the guest about your terms and conditions. The best way to do so is to send a confirmation by post, fax or e-mail listing the following details:
   – Price per overnight stay in the requested room category and invoice total (including VAT)
   – Exact hotel address
   – Reservation number
   – Information about the cancellation and debit conditions:
   **If the cardholder does not cancel the completed reservation by 6 pm local time on the scheduled arrival date, he will be billed for one night's stay (plus tax).**

### How to deal with a cancellation

You are usually obliged to accept all cancellations reaching you by 6 pm local time on the planned day of arrival. In addition, you must inform the cardholder of the cancellation number.

If this cancellation period is not long enough for you, you can set it at a maximum of 72 hours before the planned arrival of the guest. In this instance, you are obliged to inform your guest in writing about the special cancellation deadline. You should clearly state the actual date and time of this deadline in your confirmation.

If the customer fails to appear and has not cancelled the reservation, you may submit a sales draft charging the cardholder for **one overnight** stay. You should enter the comment "No show" on the signature panel. You are not entitled to compensation if the cardholder denies having made the hotel reservation himself.

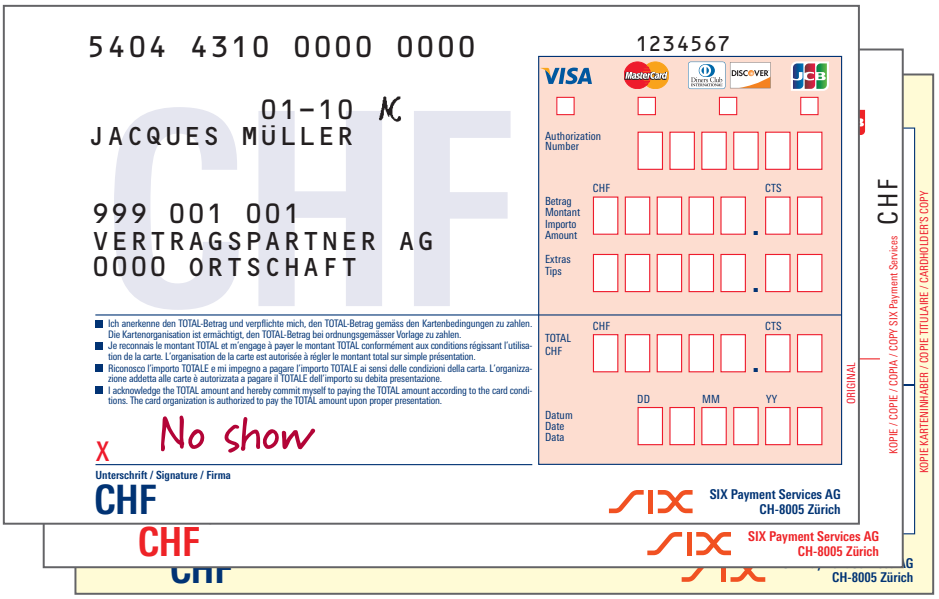
### What to do on the day of arrival

When your guest checks in, you should ask for the credit card and reserve the amount likely to be owed at the end of the stay on your terminal.

In all cases, you should read in the card on the terminal. You should not type in the card number manually un-less neither the chip nor the magnetic strip is readable and the card cannot be read in on the terminal for this reason. In this instance, you should additionally create an imprint of the card in all cases using the imprinter ("knuckle-buster") and authorise the transaction.

### Alternative accommodation

You are obliged to provide the properly reserved accommodation for your guest. If you are unable to do so, you are required to arrange comparable accommodation at the same place for him. In addition, the guest is entitled to a transfer to the alternative accommodation and a three-minute telephone call, and you are obliged to forward all messages and calls to the new accommodation free of charge.



# Hotel reservation by means of down payment with a credit card

## (Hotel Advance Deposit)

**If your hotel wishes to request an advance deposit for a guaranteed booking, this can be handled using the guest's credit card. This information sheet will tell you 1 the correct way to handle deposits paid by credit card, 2 the correct way to handle cancel deposits that have already been paid, and 3 the correct way to deal with cases of overbooking.**

**It is important for you to follow these instructions carefully. This will help to prevent queries from customers or even cancellations.**

### 1 The correct way to handle advance deposits paid by credit card

**When the guest makes the booking, you should …**

**Request the following information:**
- The cardholder's first and last name (as shown on the card)
- The invoice address
- The credit card number and expiry date
- Phone number, postal address, email address
- The arrival date and length of stay

**Give the guest the following information:**
- The room price (complete with any levies, duties, taxes)
- The amount of the advance deposit that you will charge to the credit card (this may not exceed the price for 14 nights)
- The name, address and phone number of the hotel
- The booking code[1], requesting the guest to note this number in the event of any queries
- The advice that the advance payment will be deducted from the final invoice, and
- that the accommodation will be reserved for the guest for the period covered by the advance deposit

**Inform the guest about your hotel's cancellation policy, notably**
- the last possible date for a free cancellation
- that the advance deposit will be forfeited in part or in full after the cancellation period has expired or if the cancellation policy is not observed

**After speaking with the guest …**

**Book the advance deposit on your terminal**
- As you only have the card number to hand and not the card itself, you should use the "manual data acquisition" function[2].
- You should write "Advance Deposit" in the signature field instead of the signature.

**Secure processing of the deposit in E-Commerce**
SIX Payment Services recommends our solutions; Secure PayGate or Secure E-Commerce, for processing hotel advance deposits. With Secure PayGate you proceed as follows:

1. Open Secure PayGate on your PC.
2. Open a saved standard offer or create a new individual offer.
3. Send your offer by e-mail, together with other information in the form of an attachment if you so choose (such as cancellation policy).
4. The guest reviews the offer.
5. If they agrees, they clicks on the encrypted link in the e-mail; this automatically logs him into a Saferpay payment window.
6. The guest enters his card number, card validation code (CVV2, CVC2, CID), name and date of expiration and concludes his purchase.
7. The cardholder promptly receives a confirmation of purchase by e-mail.
8. At the same time you will receive a payment confirmation by e-mail.
9. The payment is automatically filed in your back office journal where you can check and administer it.

When processing using Secure E-Commerce your guest goes on your website and follows the normal selection and payment process.

Note the following: transaction processing using manual card data acquisition is subject to risks which

[1] Assigned by the hotel
[2] The name of this function may vary according to the terminal model. Contact the manufacturer of your terminal if you have questions.

are to be borne by you as the contractual partner. This is particularly the case if it is subsequently established that the card data was misused without the cardholder's consent. In these cases you assume all risks of collecting the receivable from the cardholder for the corresponding transaction. You can significantly reduce these risks by using Secure PayGate.

**PCI DSS guidelines**
You should retain the card data in physical form and avoid storing it on a computer system. If you wish to store card data electronically, you need to be certified compliant with PCI DSS. To find out more, please refer to our instructions "PCI DSS compliance instructions Security standards for merchants". You should keep the card data recorded manually (card number and expiry date) in a secure place that is only accessible to a limited group of people. This card data must be destroyed once the guest has left the hotel. Card security numbers (CVV2, CVC2, CID, CAV2) must never be stored.

### Provide the guest with written notification of the deposit

You are obliged to send a written confirmation of the deposit to the guest together with a copy of the reservation slip within three working days.

Your hotel's deposit confirmation must include the following information[3]:
- Name of the hotel
- Name, invoice address and phone number of the cardholder
- Expected arrival date
- Amount of the deposit
- Transaction date
- Deposit booking code
- Latest cancellation date
- Cancellation policy as agreed with the guest
- Information about rights and obligations when advance deposits are paid by credit card

You must obtain written confirmation of the booking from the cardholder (by fax, letter or email). The cardholder must explicitly confirm having read, understood and accepted the cancellation policy. We recommend that you send a standard letter for the cardholder to sign and return.

## 2 The correct way to cancel advance deposits

### When talking with the cardholder

- Notify him of his cancellation code[4].
- Request him to note this code for use in the event of any queries.

### After the conversation

- Write "cancelled" and the cancellation code on the advance deposit confirmation.
- Calculate the amount to be refunded.
- Carry out a credit card refund at your credit card terminal.
- Send a copy of both slips (Advance Deposit booking slip and cancellation credit slip) to the guest within three working days by letter/fax or email together with a note explaining that a refund has been made.

Refunds may only be initiated on the same credit card that was originally debited. No other credit or debit cards, no bank transfers.

## 3 The correct way to deal with overbooking

The guest essentially has a right to the booked room or room category. If the accommodation booked by the guest is not available upon arrival, you are obliged to offer him the following services in lieu at the least:
- Accommodation in a different hotel until the reserved room is available. This must be of at least the same quality or higher.
- Transfer to the substitute hotel and back (on a daily basis, if requested by the customer)
- Forwarding of all incoming messages and calls to the substitute hotel
- Two free, three-minute phone calls
- The entire advance deposit paid by the guest must be refunded[5].

[3] Your hotel writes the confirmation of the advance deposit
[4] Your hotel assigns the cancellation code
[5] Proceed as described in section 2: The proper way to cancel down payments.

# Express Check-out

**In order to accommodate guests who are in a hurry when checking out, you can offer them the "Express Check-out" service. With this check-out variant, it is not necessary that the guest be present at reception with his or her credit card upon departure.**

**For "Express Check-out" you proceed as follows:**

– The prerequisite for the most secure possible "Express Check-out" procedure begins when checking in. Request the guest's credit card when he or she checks in and reserve the amount that it is anticipated they will owe at the end of their stay using an authorisation. It is important that you scan the card data into the terminal using a chip or magnetic strip to reserve the amount.
**Do NOT type the card data manually using the keyboard. Otherwise, in the event of complaint, the presence of the card cannot be proven.**
Furthermore, when checking in, we recommend that the guest sign a corresponding agreement (following our "Credit Card Authorisation" form), with which you can get the guest's consent when checking in to charging his or her credit card for various additional costs.

– Prepare the final bill for the guest, including restaurant, telephone and other costs. Compare the amount on the final bill with the total amount of all authorised estimated amounts:
  – If the amount on the final bill is less than the total of all amounts previously authorised plus 15 percent, no further authorisation is needed.
  – If the amount of the final bill is more than 15 percent above the total amount of all amounts previously authorised, then authorisation for the remaining difference is mandatory.
  – If no authorisation was obtained beforehand, the entire amount must be authorised.

– Note "Signature on File" on the transaction receipt in the signature field.

– Within three working days after the "Express Check-out", send the cardholder all transaction information:
  – Copy of the terminal/transaction receipt
  – Detailed hotel bill with breakdown of costs
  – Copy of the "Credit Card Authorisation" form showing the credit card charged.

Please ensure that you do not send the guest the "Credit Card Authorisation" form by e-mail and that before scanning the card you blank the card number except for the last 4 digits (compliance with security regulations in accordance with PCI DSS).

– Keep all these documents locked away for at least 3 years, as required by local legislation.

The "Express Check-out" poses a latent financial risk. If it subsequently becomes apparent that the card which was used was deployed in an improper manner and/or not by the cardholder, he or she can claim back the wrongfully booked amount. For this reason, we recommend that you offer the "Express Check-out" procedure only to guests you know. For new or first-time customers, it is recommended that you apply the normal check-out procedure or carry out the procedure on the evening prior to departure.

# Late Charges

**If you determine after the guest has checked out that additional costs have been generated which are not accounted for in the final bill (for example room service, telephone or minibar), you can retroactively charge the credit card with these additional costs.**

This requires that you explain the General Terms and Conditions as relates to additional costs to the customer when he or she is checking in. For this reason we recommend that you have the guest sign a corresponding agreement (following our "Credit Card Authorisation" form) already when checking in.

If the customer has given his consent to charging additional costs in this way, submit a separate transaction receipt for the costs determined subsequently, noting "Signature on File" in the signature field.

- Type in the credit card number given in the agreement using the terminal keyboard and charge the additional costs determined.
- If the attempt to charge does not succeed (authorisation refused), contact the cardholder and request a different means of payment.
- If the charging can be concluded successfully, note "Signature on File" on the signature line of the terminal receipt; retain it and add it to the documents related to the hotel guest.
- Send the cardholder information on the additional costs:
  - Copy of the transaction receipt with the note "Signature on File" in the signature field
  - Copy of the transaction documents with a detailed breakdown of the additional costs

**PCI DSS guidelines**
Observe the guidelines of the security standard defined by the leading card organisations: PCI DSS. You will find explanations on page 10 of this handbook.

Additional costs charged retroactively may only relate to rooms, meals or drinks. The hotel bill may increase this additional entry by a maximum of 15%.
If the additional costs total more than 15% or if costs are incurred due to loss, theft or damage in the hotel room, these can only be charged retroactively if you have contacted the guest after his departure once again and agreed this with him or her. Consent that these costs may be charged to the card must be in writing.

# Effective card data protection thanks to the security standard PCI DSS

**More and more people appreciate the flexibility and the independence of paying with credit and debit cards. And more and more hotels and restaurants are pleased with the growing card revenue. It is important to heed several security precautions so that your business remains untroubled. The PCI security standard provides appropriate principles to reduce the risks that lie in wait for the card business.**

**The Payment Card Industry Data Security Standard,** PCI DSS for short, is a set of rules in electronic payment transactions that relates to secure processing of card transactions; compliance with it is a mandatory requirement from the leading card organisations – Visa, MasterCard, JCB International, American Express and Discover Financial Services. The set of rules was issued and further developed by the PCI SSC (Payment Card Industry Security Standards Council).

All companies that store, transmit or process card data must fulfil the security principles of this set of rules. If the requirements are not complied with, the card organisations can ultimately disallow acceptance of card payments.

The purpose of the set of rules is to protect you against the undesired consequences of card data theft; besides incurring financial losses, a loss of card data is accompanied by reputational damage.

The set of rules consists of a list of twelve requirements and relates to your hotel's IT infrastructure, processes and employees:

1. Installing and maintaining a firewall to protect card data
2. Changing passwords and other security settings after delivery from the factory (e.g., replacing default passwords with personal passwords)
3. Protecting stored card data
4. Transmitting encrypted card data over public networks
5. Using and regular updating antivirus protection programmes
6. Developing and maintaining secure systems and applications
7. Restricting access to card data depending on business need for information
8. Assigning a unique identifying code for each person with access to the computer
9. Restricting physical access to card data
10. Logging and checking all visitors accessing networks and card data
11. Regularly checking on all security systems and processes
12. Launching and complying with guidelines relating to information security for employees and service providers

Compliance with the guidelines is checked using three different validation measures:

– Hotels with more than 6 million transactions a year, or contractual partners who were victims of card data theft, conduct an on-site audit. This must be conducted by a trained auditor or an accredited certification company (**QSA –** Qualified Security Assessor).
– For hotels with fewer than 6 million transactions a year, compliance with the guidelines can be declared using an **SAQ,** a Self Assessment Questionnaire. There are specific versions of this SAQ document depending on the form of card acceptance.
– For hotels whose infrastructure comes into contact with card data, there are also so-called network scans. On a quarterly basis and upon arrangement with you, an ASV (Approved Scanning Vendor) will carry out friendly hacking attacks. The aim is to determine vulnerabilities in the network in a timely manner.

# Resources

**As a basic principle, the best solutions are those in which your company does not even come into contact with complete, unencrypted card data. If you can ensure this, the expense of certification is considerably reduced.**

**The following resources help you reduce the risk and expense of certification.**

## PCI Proxy Server

The Internet is used extensively these days as an additional sales channel. In this respect, hotel reservation platforms provide significant support. Unfortunately, complete card data are often sent out in unencrypted form via e-mail or XML interface when using reservation platforms.

Receiving this card data in clear text dramatically increases the number of security guidelines to be complied with for the PCI DSS. So that,despite this way of working together,you need not go without a reduced certification approach, SIX Payment Services conducted a number of discussions with the company Datatrans and helped design a PCI proxy solution.

Here the proxy server from Datatrans switches between the reservation platform and your company for the booking information with card data that is transmitted via e-mail or by XML interface. In so doing the card data is encrypted and saved in Datatrans's secure environment; you will receive only a reference number. In this way, your hotel does not come in contact with these card data, but you nonetheless have the possibility to charge the guest's credit card by using a reference number.

For further information please contact Datatrans directly: www.datatrans.ch or info@datatrans.ch

## Hotel Software – Property Management System (PMS)

Ensure that your hotel software is certified according to PA-DSS (Payment Application Data Security Standard) and has a reference number module (with which the encrypting of the card data is carried out by the PMS software).

Contact your software provider and have him certify your PA-DSS conformity.

## Foregenix Tool

If you are not sure whether there are card data in your infrastructure, the company Foregenix offers you valuable support with the tool "FScout". This tool scans your entire infrastructure for card data. If the tool discovers any, you can have the files found isolated or deleted. In this way you can ensure there are no hidden files with card data in your infrastructure.

You will find more information on the homepage of Foregenix: www.foregenix.com

## SAQ Web portal

SIX Payment Services operates a Self-Assessment Questionnaire (SAQ) web portal in cooperation with Acertigo GmbH.

This portal supports you in executing all steps necessary for PCI DSS to obtain a PCI certification and renew it on a regular basis. The portal offers a comfortable user interface which leads you step by step through all necessary certification processes.

In the portal's document archive all documents incurred during execution are stored for the dealer and can be reviewed online or downloaded. This includes, for instance, the completed SAQ, the results of the network scans and the certification confirmations.

You can register at the portal free of charge and conduct classification to determine the necessary certification steps.

If you have technical or content-related questions you can directly contact the PCI team:
pci-support@six-group.com or by telephone at
0041 (0)58 399 9955.

## Secure PayGate

If you accept reservations by telephone, fax, e-mail or by mail, your guests can pay their accommodation costs quickly, comfortably and securely in advance without your hotel coming into contact with card data. The solution is called Secure PayGate.

Secure PayGate links the advantages of the so-called mail/phone order transaction with the security of a password-protected Secure E-Commerce transaction. For you this means: more security and better conditions.

You will find more information about Secure PayGate at: www.saferpay.com

## PCI Hotel Checklist

Are you uncertain whether and to what extent there is a risk of card data theft in your hotel? Then fill out the checklist on the next pages and send it to:

SIX Payment Services, PCI Compliance, Hardturmstrasse 201, P. O. Box, CH-8021 Zurich

We will contact you should our specialists identify a security vulnerability.

Payment Services

# PCI Hotel Checklist

Hotel name: _____

Address: _____

Contact person: _____

Partner ID: _____

Client advisor: _____

| | Yes | No |
|---|---|---|
| Is the hotel already PCI DSS certified or in the process of becoming certified? | ☐ | ☐ |

Expected compliance date: _____

## PCI-sensitive processes

| | | |
|---|---|---|
| Are late charge bookings possible? | ☐ | ☐ |
| Are no-show bookings possible? | ☐ | ☐ |

*If you answered yes to one of these questions, please answer the additional questions under "Detailed Questions" below.*

## Reservation platforms

| | | |
|---|---|---|
| Does the hotel work together with a hotel reservation platform and/or does the hotel run its own reservation platform? | ☐ | ☐ |

*If you answered yes to this question, please enter the reservation platforms used under "Detailed Questions" below.*

## Reservations by post, fax, telephone or e-mail

| | | |
|---|---|---|
| Are reservations accepted by post, fax or telephone? | ☐ | ☐ |
| Are reservations accepted by e-mail? | ☐ | ☐ |

*If you answered yes to one of these questions, please answer the additional questions under "Detailed Questions" below.*

## Infrastructure – optional

| | | |
|---|---|---|
| Are records kept which allow external employees to be identified and which contain exact times of stay or locations? | ☐ | ☐ |
| Are all paper documents containing card data kept in a locked room or safe and marked as "confidential"? | ☐ | ☐ |
| Do guests' payment and reservation records contain only masked card data? | ☐ | ☐ |
| Are paper documents containing card data shredded when no longer needed? | ☐ | ☐ |
| Is the fax machine on which reservations containing card data are received kept in a secure environment? *(Secure environment: Access only for authorized persons, or 24/7 surveillance of the fax machine, for example by receptionists)* | ☐ | ☐ |

## Employees – optional

| | | |
|---|---|---|
| Do all employees who come into contact with card data sign a data protection agreement? | ☐ | ☐ |
| Are all employees who need to have access to card data for business reasons sensitized to the protection of such data? | ☐ | ☐ |
| Do only those employees needing card data to carry out their business activities have access to areas where card data is stored? *(Areas with card data: Offices with fax machines and computers connected to PMS or POS systems as well as archives containing credit card receipts)* | ☐ | ☐ |

# Hotel Checklist – Detailed Questions

## PCI-sensitive processes

| Additional questions about express checkout, late charge and no-show bookings | Yes | No |
|---|---|---|
| Are the card data needed for express checkout, late charge or no-show bookings temporarily electronically stored until the booking is carried out? | ☐ | ☐ |
| *If yes* | | |
| Are the electronic card data temporarily stored in a PCI-certified application? | ☐ | ☐ |
| *or* | | |
| Are the card data needed for express checkout, late charge or no-show bookings temporarily stored on paper until the booking is carried out? | ☐ | ☐ |
| *If yes* | | |
| Are the card data on paper stored in a secure environment? *(Secure environment: Access only for authorized persons and storage areas that can be locked)* | ☐ | ☐ |

## Reservation platforms

We work with the following reservation platforms

☐ **Booking.com**

Contact person:

☐ **Expedia.de**

Contact person:

☐ **HRS.com**

Contact person:

☐ **Swisshotels.ch**

Contact person:

☐ Name:

Contact person:

☐ Name:

Contact person:

| | Yes | No |
|---|---|---|
| Do you receive e-mails containing customer card data from the reservation platforms? | ☐ | ☐ |
| *If yes* | | |
| Are the e-mails encrypted for transmission? | ☐ | ☐ |
| Are the e-mails deleted after use (including emptying the recycle bin)? | ☐ | ☐ |
| Does the hotel run its own reservation platform on the Internet? | ☐ | ☐ |
| Is the software used PCI compliant? | ☐ | ☐ |

Manufacturer:

Contact person:

Software:

Phone number:

## Reservations by post, fax, telephone or e-mail

*When reservations are made by fax or telephone, the merchant/hotelier bears the financial risk for payments booked fraudulently using cards or card data.*

| | | |
|---|---|---|
| When reservations are received by post, fax or telephone, are card data written down on paper? | ☐ | ☐ |
| *If yes* | | |
| Are these card data kept in a secure environment? *(Secure environment: Access only for authorized persons and storage areas that can be locked)* | ☐ | ☐ |
| When reservations are received by fax or telephone, are the card data recorded electronically? | ☐ | ☐ |
| *If yes* | | |
| Are the card data stored temporarily in a PCI certified application? (for example Alias Module) | ☐ | ☐ |

*E-mail orders containing complete card numbers or data are generally not permitted. The following questions apply if you receive an unsolicited e-mail with card data in plain text.*

| | | |
|---|---|---|
| Are e-mails containing card data printed and deleted following receipt – including emptying the recycling bin? | ☐ | ☐ |
| Are the printed e-mails archived in a secure environment? *(Secure environment: Access only for authorized persons and storage areas that can be locked)* | ☐ | ☐ |

Place and date

First name and last name

Signature of merchant

Your personal contact: www.six-payment-services.com/contact

**SIX Payment Services Ltd**
Hardturmstrasse 201
8005 Zurich
Switzerland

**SIX Payment Services (Europe) S.A.**
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

# Credit card authorisation (sample)

Below you will find a sample form with which you can have your guests authorize bookings without the card itself being present (express check-out, late charges, additional services):

Your hotel name / your hotel logo: _____

**This form must be kept in a secure environment.**

## Kreditkarten-Autorisierung / Credit card authorization

Karteninhaber /
Credit card holder _____ Zimmer / Room _____

☐ Zahlung / Payment
*oder / or*
☐ Garantie / Guarantee

Kartentyp / Type ☐ Visa ☐ MasterCard ☐ American Express ☐ Diners ☐ JCB ☐ UnionPay

Nummer / Number _____ Verfallsdatum / Expiration _____

**Für folgende Services / For the following charges**

Zimmer und Taxen / Room and tax ☐
Express Check-Out / Express check-out ☐
Frühstück / Breakfast ☐
Übrige Gebühren / All incidentals ☐

**Für folgende Gäste / For the following guests**

Name / Name _____ Zimmer / Room _____
Name / Name _____ Zimmer / Room _____
Name / Name _____ Zimmer / Room _____

Hiermit bestätige ich, dass nebst meiner Zimmerrechnung auch die auf diesem Formular markierten Zusatzkosten sowie die Zimmerrechnung für die anderen aufgeführten Gäste gemäss den allgemein gültigen Geschäftsbedingungen unseres Hauses zu Lasten meiner oben erwähnten Kreditkarte abgebucht werden dürfen.

I hereby confirm that, excepting my room costs, the additional costs marked above and room costs for the other guests listed on this document can be charged to my above mentioned credit card in accordance with the general business terms and conditions.

_____ _____
Ort, Datum / Place, date Vorname, Name / Nom First name, last name

_____
Unterschrift / Signature

Your personal contact: www.six-payment-services.com/contact

**SIX Payment Services Ltd**
Hardturmstrasse 201
8005 Zurich
Switzerland

**SIX Payment Services (Europe) S.A.**
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

# Data protection agreement (sample)

**Below you will find a non-binding example of a possible data protection agreement. For a legally binding version, please contact a lawyer of your choice.**

On the basis of contractual and statutory confidentiality obligations, the undersigned is required to maintain confidentiality about the facts/information which he or she has attained or become aware of by working at *Hotel Musterhof;* facts/information, that is, which are not generally known, where an interest in its confidentiality is worthy of protection and about which maintaining confidentiality is expressly or tacitly the will of *Hotel Musterhof.*

– Any information relating to the subject, contents and function of the technical or software-supported resources and equipment of *Hotel Musterhof* as well as relating to the organization and processing of all types of business at the *Hotel Musterhof* is covered by the obligation of professional secrecy.
– All personal customer data, including credit or debit card data, are to be especially protected.

Contravening the confidentiality obligation can represent individually or cumulatively a breach of the obligation of professional secrecy or the law on data protection. The corresponding legal provision is reproduced in the appendix to this declaration of confidentiality.

The undersigned commits to treat in strict confidentiality facts/information of which he or she has become aware that are relevant to confidentiality and to use them for no other purpose than for the task for which they were entrusted to him or her.

Place and date

Name of the person signing

Signature

**Appendix**

Art. 162 Violation of Trade or Business Secrets
If an individual reveals a trade or business secret that he should keep as a consequence of a legal or contractual obligation, if an individual exploits this betrayal for himself or another, he or she will be punished upon application by a term of imprisonment of up to three years or by a monetary penalty.

110.0116.02 CHE_EN/09.2013

Your personal contact: www.six-payment-services.com/contact

**SIX Payment Services Ltd**
Hardturmstrasse 201
8005 Zurich
Switzerland

www.six-payment-services.com

Feedback, comments, suggestions and proposals about this brochure to:

PCI Compliance
T 058 399 9955

pci.ch@six-payment-services.com