Conditions for the Debit Cards

I. Applications related to payment transactions

1. Range of applications

1.1 For payment transactions

The cardholder may use the Visa or Mastercard debit card (hereinafter referred to as the "Debit Card") issued by solarisBank AG (hereinafter referred to as the "Bank") in Germany and, as an additional service, abroad within the Visa or Mastercard network

- for payments ~~with~~ at contracting companies on site at automated cash registers and online and
- in addition, as a further service, to withdraw cash from cash machines and from financial institutions on presentation of an appropriate identification document (cash service).

The contracting companies and the financial institutions and cash machines participating in the cash service can be identified by the acceptance symbols that also appear on the Debit Card. If the Debit Card is associated with additional services (assistance in emergencies, for example, or insurance policies), these are governed by the applicable special regulations.

The Debit Card can be issued as a physical card or as a digital card for storage on a telecommunication, digital or IT device (mobile terminal). These special conditions apply equally to both types of Debit Cards, unless expressly provided otherwise. For the digital card, the terms of use for the digital card agreed separately with the Bank shall apply in addition.

If the Debit Card has been issued as a business card, it may be used exclusively for business purposes.

1.2 As a storage medium for additional applications

If the Debit Card issued to the cardholder has a chip, the Debit Card may be used as a storage medium for additional applications

- of the Bank that issues the Debit Card in accordance with the contract concluded with the Bank (bank-generated additional application) or
- of a contracting company in accordance with the contract concluded with the latter (company-generated additional application).

2. Personal identification number (PIN)

The cardholder shall be issued with a personal identification number (PIN) for use in cash machines and at automated checkouts with his Debit Card.

If the PIN is entered incorrectly three times in succession, the Debit Card can no longer be used in cash machines and at automated checkouts in which the PIN must be entered to use the Debit Card. In this case, the cardholder should contact the partner of the bank who provides the user interface.

3. Authorisation of card payments by the cardholder

(1) When using the Card, either

- a receipt on which the contracting company has entered the Debit Card details must be signed or
- the PIN must be entered at cash machines and automated checkouts.

After prior consultation between the cardholder and the contracting company, the cardholder may exceptionally refrain from signing the receipt - in particular to speed up a business transaction within the framework of a telephone contact - and instead merely state his debit card number.

When the Debit Card is used at automated cash registers, it is not necessary to enter the PIN:

- For payment of traffic usage fees or parking fees at unattended automated checkouts.
- For contactless payment of small amounts. The Debit Card with contactless function must be held against a card reader. The amount and usage limits specified by the Bank apply.

For online payments, the cardholder is authenticated by using the separately agreed authentication elements on request. Authentication elements are

- Knowledge elements (something the cardholder knows, for example, an online password),

- Possession elements (something that the cardholder possesses, for example, mobile device for the generation of a one-time usable transaction number (TAN) as proof of possession) or

- Being elements (something that is the cardholder, for example fingerprint).

~~In the case of contactless payment, the Debit Card with contactless function must be held against a card reader. In this case, signature of the receipt or entry of the PIN on a card payment terminal is required only above an amount specified by the body accepting the Debit Card and is not otherwise necessary.~~

~~With prior agreement between the cardholder and contracting company, the cardholder may exceptionally – and in particular to speed up a business transaction – not be required to sign the receipt but simply provide his card number instead.~~

(2) By using the Card, the cardholder is giving consent (authorisation) to complete the card payment. If, in addition, a PIN or signature is required for this, consent is given only when this is provided. Once consent has been given, the cardholder cannot cancel the card payment. The authorisation also includes the express consent that the Bank processes, transmits and stores the personal data of the cardholder which is necessary for the execution of the card payment.

4. Blocking of an available amount of money

The Bank shall be entitled to block an amount of money available on the cardholder's account within the limits of the financial limit of use (cf. number 7) if

- the payment transaction has been triggered by the payee and
- the cardholder also agrees to the exact amount of the amount of money to be blocked.

Without prejudice to any other legal or contractual rights, the Bank shall release the exact amount of money without delay after having been notified of the exact payment amount or after the payment order has been received.

5. Rejection of card payments by the Bank

The bank is entitled to reject the card payment if

- the cardholder has not confirmed it with his PIN,
- the transaction limit for card payments that applies to the Debit Card or the financial usage limit has not been observed,
- there is a suspicion of unauthorised or fraudulent use of the Debit Card, or
- the Debit Card is blocked.

The cardholder will be informed of this via the terminal at which the Debit Card is being used or in the case of online use on the agreed way.

6. Completion period

The payment process is triggered by the payee. On receipt of the payment order by the Bank, the latter is obliged to ensure that the card payment amount is received by the payee's payment service provider at the latest by the time specified in the "List of Prices and Services".

7. Financial usage limit

The cardholder may use the Debit Card only within the credit available in the agreed payment account or within the transaction limit of the Card, and only in such a way that settlement of the card transactions is ensured when they become due. The cardholder may agree a change to the transaction limit of the Debit Card with his bank.

Even if the cardholder does not comply with the financial usage limit, the Bank is entitled to demand reimbursement of the expenses that arise from use of the Debit Card. Approval of individual card transactions does not entail either the provision of credit or an increase of a credit amount previously agreed, but is given in the expectation that settlement of the card transactions is guaranteed when they become due.

If the booking of the card transactions exceeds the existing account balance or a credit limit previously agreed, the booking shall lead to a tolerated overdraft.

8. Cardholder's duty of care and cooperation obligations

8.1 Signature

On receipt of his Card, the cardholder shall sign the signature strip immediately.

8.2 Safekeeping of the Card

The Debit Card must be kept safe with particular care in order to prevent it from being lost or misused. In particular, it must not be kept unattended in a vehicle. Anyone who is in possession of the Debit Card is able to use it for improper transactions.

8.3 Confidentiality of the ~~personal identification number (~~PIN~~)~~

The cardholder shall ensure that no one else gains knowledge of his personal identification number (PIN). In particular, it must not be written on the Debit Card or otherwise kept with it. Anyone who gains knowledge of the PIN and comes into possession of the Debit Card is able to carry out improper transactions with the PIN and Debit Card (withdraw cash from cash machines, for example).

8.4 Protection of authentication elements for online payments

The cardholder shall take all reasonable precautions to protect his online payment authentication elements agreed with the Bank (see point 3(1) last subparagraph of these conditions) from unauthorised access. Otherwise, there is a risk that the authentication elements for online transactions may be misused or otherwise not authorised.

In order to protect the individual authentication elements for online payment transactions, the cardholder shall pay particular attention to the following:

(a) Knowledge elements, such as the online password, shall be kept secret; they may in particular
  - not be communicated orally (e.g. by telephone or in person),
  - not be passed on outside of online payment transactions in text form (e.g. by e-mail or messenger service),
  - are not be stored unsecured electronically (e.g. storage of the online password in plain text on the mobile device), and
  - not be recorded on a device or stored as a transcript together with a device which serves as a possession element (e.g. mobile device) or for checking the being element (e.g. mobile device with application for card payment and fingerprint sensor)

(b) Possession elements, such as a mobile device, shall be protected from misuse, in particular
  - it must be ensured that unauthorised persons cannot access the cardholder's mobile device (e.g. mobile telephone),
  - it must be ensured that other persons cannot use the card payment application on the mobile device (e.g. mobile phone) (e.g. card app, authentication app),
  - the application for online payment transactions (for example card app, authentication app) on the mobile device of the subscriber must be deactivated before the subscriber gives up possession of this mobile device (e.g. by selling or disposing of the mobile phone), and
  - the proofs of ownership (e.g. TAN) may not be passed on orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service) outside the online payment processes.

(c) Being elements, such as the cardholder's fingerprint, may only be used as an authentication element on a mobile terminal of the cardholder for online payment transactions if no other person's elements of being are stored on the mobile device. If the mobile device used for online payment transactions stores the identity elements of other persons, the knowledge element issued by the bank (e.g. online password) is to be used for online payment transactions and not the identity element stored on the mobile device.

8.5 Control obligations for online payment transactions

If, in the case of online payment transactions, the cardholder is notified of details of the payment transaction (e.g. the name of the contracting company and the amount of the transaction), the cardholder must check this data for correctness.

~~8.4~~8.6 Cardholder's notification and reporting obligations

(1) If the cardholder becomes aware of the loss or theft of his Card, its improper use or any other unauthorised use of the Debit Card or the PIN, the Bank, if possible, the branch at which the account is held, or a representative office of the Visa or Mastercard network shall be notified immediately to arrange for the Debit Card to be blocked. The cardholder shall be notified separately of the contact details for submitting a blocking notification. The cardholder shall report any theft or misuse to the police immediately.

(2) If the cardholder suspects that someone else has come into possession of his Debit Card illegitimately, it is being used improperly or any other unauthorised use of the Debit Card or PIN is being made, he shall immediately submit a blocking notification in the same way.

(3) If the Debit Card has a TAN generator or a signature function ~~for online banking~~, blocking the Debit Card also results in blocking access to online banking.

(4) Blocking of a company-generated additional application can only be carried out by the company that has saved the additional application to the chip on the Debit Card and is only possible if the company has provided the option to block its additional application. Blocking of a bank-generated additional application can only be carried out by the card-issuing bank and is governed by the contract concluded with the card-issuing bank.

(5) The cardholder shall notify the Bank as soon as an unauthorised or erroneous card transaction is identified.

9. Payment obligation of the cardholder

The Bank is obliged to settle the transactions carried out by the cardholder with the Debit Card in respect of contracting companies and financial institutions that accept the Debit Card in their cash machines.

The transactions carried out with the Debit Card shall be charged to the agreed payment account on the day of receipt by the Bank. The Bank shall inform the cardholder at least once a month of all expenses associated with settlement of the card transactions, by the method agreed for providing account information. For cardholders who are not consumers, the method and timing of such notification shall be agreed separately.

Objections and other complaints by the cardholder arising from the contractual relationship with a contracting company with which the Debit Card was used shall be pursued directly with that contracting company.

10. Foreign currency conversion

If the cardholder uses the Debit Card for transactions that are not in euros, the account shall still be charged in euros. The exchange rate for foreign currency transactions shall be determined on the basis of the Bank's "List of Prices and Services". A change to the reference exchange rate specified in the conversion regulation shall take effect immediately and without prior notification of the cardholder.

11. Fees

(1) The fees owed by the cardholder to the Bank shall be determined on the basis of the Bank's "List of Prices and Services".

(2) Changes to the fees shall be proposed to the cardholder in written form no later than two months before they are to take effect. If the cardholder has agreed an electronic means of communication with the Bank as part of the business relationship (online banking, for example), the changes may also be proposed by this means. The cardholder may either agree or reject the changes before the proposed date of entry into force. The cardholder is deemed to have consented if he fails to provide notice of his rejection in advance of the proposed date of the changes coming into effect. The Bank shall make specific reference to this de facto consent in its offer.

(3) When the cardholder is notified of changes to the fees, he may cancel the business relationship without notice and at no cost in advance of the proposed date of the changes coming into effect. The Bank shall make specific reference to this right to terminate in its offer.

(4) In the case of fees and changes to them for payments by cardholders who are not consumers, the regulations in number 12 paragraphs ~~.~~ 2 to ~~.~~ 6 of the Bank's General Terms & Conditions apply.

12. Cardholder's entitlement to reimbursement and compensation

12.1 Reimbursement for unauthorised card transaction

In the case of an unauthorised card transaction in the form of

- a withdrawal of cash or
- use of the Debit Card with a contracting company

the Bank does not have any claim against the cardholder for reimbursement of its expenses. The Bank is obliged to reimburse the user with the amount immediately and in full. If the amount has been debited from an account, the Bank shall restore it to the balance that it would have had if the unauthorised card transaction had not taken place. In accordance with the "List of Prices and Services", this obligation must be fulfilled no later than the end of the business day following the day on which the Bank was notified that the transfer is unauthorised or has otherwise learned thereof. If the Bank has in-formed a competent authority in writing of justified grounds for suspecting fraudulent conduct on the part of the cardholder, the Bank must examine its obligation under sentence 2 without delay and fulfil this obligation when the suspicion of fraud is not confirmed.

12.2 Claims for non-execution, incorrect or belated execution of an authorised card transaction

(1) In the event of non-executed or incorrect processing of an authorised card transaction in the form of

- a withdrawal of cash or
- use of the Debit Card with a contracting company,

the cardholder may demand immediate and full reimbursement of the transaction amount insofar as the card transaction failed to take place or was incorrect. If the amount has been debited from

an account, the Bank shall restore it to the balance that it would have had if the failed or incorrect card transaction had not taken place.

(2) In addition to paragraph 1, the cardholder may demand reimbursement by the Bank of any fees or interest that were charged to him or debited from his account in connection with the authorised card transaction that failed to take place or was processed incorrectly.

(3) If the payment amount is received by the payee's payment service provider only after expiry of the execution period specified under number 6 (delay), the payee may require his payment service provider to credit the payment amount to the payee's account as if the card payment had been duly executed.

(4) If an authorised card transaction failed to take place or was processed incorrectly, the Bank shall at the request of the cardholder investigate the card transaction and report the findings to him.

12.3 Compensation claims by the cardholder on the basis of an unauthorised card transaction or non-executed, incorrect or belated processing of an authorised card transaction

In the case of an unauthorised card transaction or in the case of a non-executed, incorrect or belated processing of an authorised card transaction, the cardholder may demand compensation from the Bank for losses not already covered under Numbers 12.1 and 12.2. This does not apply if the Bank was not responsible for the breach of obligation. In this context, the Bank is responsible for obligations incurred by an intermediary that it has appointed as if they had been incurred by the Bank itself, unless the main cause was the responsibility of an intermediary specified by the cardholder. If the Debit Card is used in a country outside Germany and the European Economic Area, the liability of the Bank for the culpability of a body involved in processing the payment transaction is restricted to the careful selection and training of such a body. If the cardholder has contributed to the occurrence of a loss through culpable conduct, the principles of contributory culpability shall determine the extent to which the Bank and the cardholder shall bear the loss. Liability under this paragraph is limited to EUR 12,500 per card transaction. This limitation to the amount of liability does not apply

- to unauthorised card transactions,
- in the event of malicious intent or gross negligence on the part of the Bank,
- to risks that the Bank has specifically taken on, and
- to losses of interest incurred by the cardholder if the cardholder is a consumer.

12.4 Period for pursuit of claims under numbers 12.1 to 12.3

Claims against the Bank in numbers 12.1 to 12.3 are excluded if the cardholder has not notified the Bank that a card transaction is unauthorised, has not been completed or is incorrect at the latest 13 months from the date on which the card transaction was charged. The 13-month notification period commences only when the Bank has notified the user of booking of the charge resulting from the card transaction by the agreed means, at the latest within a month of booking of that charge; otherwise, the day of such notification shall determine commencement of the period. Claims for liability under number 12.3 may still be pursued by the cardholder after expiry of the notice period under sentence 1 if he was unable to meet the deadline for reasons beyond his control.

12.5 Claim for reimbursement in the event of an authorised card transaction without a specific amount and period for pursuit of the claim

(1) The cardholder may demand immediate and full reimbursement of the transaction amount if he has authorised a card transaction with a contracting company in such a way that

- the exact amount was not specified on authorisation and
- the payment process exceeds the amount that the cardholder could have expected given his previous spending behaviour, the content of the card contract and the relevant circumstances of the individual case; reasons related to any currency conversion cannot be considered if the agreed reference exchange rate was used as the basis.

The cardholder is obliged to explain the facts of the situation on which the claim for reimbursement is based to the Bank.

(2) The claim for reimbursement is excluded if it has not been pursued with the Bank within eight weeks of the date on which the transaction was charged to the payment account.

12.6 Exclusion of liability and objection

Claims of the cardholder against the Bank under Numbers 12.1 to 12.5 are excluded if the circumstances on which a claim is based

- result from on an unusual and unforeseeable event over which the Bank has no influence, and the consequences of which could not have been avoided despite exercising due care, or
- are brought about by the Bank as the result of a statutory obligation.

13. Liability of the cardholder for unauthorised card transactions

13.1 Liability of the cardholder until the blocking notification

(1) If the cardholder misplaces his Debit Card or PIN, they are stolen from him or lost or the Debit Card, PIN or or the authentication instruments agreed for online payment transactions are otherwise misused and, as a result, unauthorised card transactions are carried out in the form of

- a withdrawal of cash or
- use of the Debit Card with a contracting company,

the cardholder is liable for losses incurred up to the blocking notification, up to a maximum of EUR 50, irrespective of whether the cardholder is to blame for the loss, theft or other loss or other misusebut not if the misplacement, theft or other loss of the Debit Card is not the responsibility of the cardholder, the cardholder is not culpable or it is merely the result of minor negligence.

(2) The cardholder shall not be liable in accordance with paragraph 1 if

- it has not been possible for him to notice the deprivation, theft, loss or any other misuse of the card or the mobile device with the digital card prior to the unauthorised payment process, or

- the loss of the card has been caused by an employee, an agent, a branch of a payment service provider or a body to which the Bank's activities have been outsourced.

(3) If the cardholder is not a consumer or the Debit Card is used in a country outside of Germany and the European Economic Area, the cardholder shall be liable for the damage resulting from an unauthorized card order pursuant to paragraph~~s~~ 1 in excess of a maximum of EUR 50~~and 2~~, if the cardholder has negligently breached the obligations incumbent upon him under these terms and conditions. If the Bank has contributed to the occurrence of damage through a breach of its obligations, the Bank shall be liable for the resulting damage to the extent of contributory negligence for which it is responsible.

(4) If unauthorised transactions are carried out before the blocking notification and the cardholder has acted with fraudulent intent or breached his duty of care as specified in these conditions intentionally or as a result of gross negligence, the cardholder is responsible for the resulting losses in full. Gross negligence of the cardholder may exist, in particular, if

- he has culpably failed to notify the Bank or a representative office of VISA or Mastercard~~the Debit Card company~~ immediately after he becomes aware of the loss, theft or improper use of the Dbeit Card,
- the personal identification number or the agreed knowledge element for online payment transactions (e.g. online password) has been written on the Debit Card or has been kept with the Debit Card (in the form of the original letter in which it was communicated to the cardholder, for example),
- the personal identification number or the agreed knowledge element for online payment transactions (e.g. online password) has been communicated to another person and the misuse has resulted from this.

(~~4~~5)Liability for losses incurred within the period to which the transaction limit applies are restricted in each case to the transaction limit applicable to the Debit Card.

(~~5~~6)The cardholder shall not be obliged to pay compensation for the damage in accordance with paragraphs 1, 3 and 4 if the cardholder was unable to report the blocking notice because the Bank had not secured the possibility of accepting the blocking notice.

(~~6~~7)If the Bank did not require strong customer authentication in accordance with Section 1 (24) of the Payment Services Supervision Act [*Zahlungsdiensteaufsichtsgesetz, ZAG*] when using the Debit Card for payments on the Internet or if the creditor or his payment service provider did not accept this, although the Bank was obliged to provide strong customer authentication according to Section 55 ZAG, the liability of the cardholder and the Bank shall be determined in deviation from paragraphs 1, 3 and 4 of this article in accordance with the provisions of Section 675v (4) of the German Civil Code [*Bürgerliches Gesetzbuch*], BGB. Strong customer authentication requires in particular the use of two independent elements from the categories knowledge (something the participant knows, e. g. PIN), ownership (something the participant possesses, e. g. TAN generator) or inherence (something the participant is, e. g. fingerprint).

(~~7~~8)Paragraphs 2 and 5 to 7 shall not apply if the cardholder has acted with fraudulent intent.

13.2 Liability of the cardholder after the blocking notification

As soon as the loss or theft of the Card, its improper use or any other unauthorised use of the Card, PIN or personalised security feature has been reported to the Bank or a representative office of the Debit Card company, the Bank is responsible for all subsequent losses in the form of

- a withdrawal of cash or
- use of the Debit Card with a contracting company.

If the cardholder acts with fraudulent intent, the cardholder is also responsible for losses incurred after the blocking notification.

14. Joint and several liability of multiple applicants

The applicants are liable for the obligations arising from a joint Debit Card as joint and several debtors, i.e. the Bank may demand settlement of all claims from each applicant.

Each applicant may end the contractual relationship by termination at any time with effect for all applicants.

Each applicant shall ensure that the Debit Card issued to him is returned to the Bank immediately when the termination comes into effect. The applicants shall likewise bear the costs incurred from further use of a Debit Card until its return to the Bank as joint and several debtors. Irrespective of this, the Bank shall take reasonable measures to prevent card transactions following termination of the contractual relationship for the card.

15. Ownership and validity of the Card

The Debit Card shall remain the property of the Bank. It is non-transferable. The Debit Card is valid only for the period specified on the Debit Card.

The Bank is entitled to demand return of the old Debit Card when a new Debit Card is issued, at the latest on expiry of its validity. If the right to use the Debit Card ends before this (by termination of the Debit Card contract, for example), the cardholder shall return the Debit Card to the Bank immediately. The cardholder shall arrange for additional company-generated applications on the Debit Card to be removed without delay by the company that set up the additional application on the Debit Card. The option to continue using a bank-generated additional application is governed by the contractual relationship between the cardholder and the card-issuing Bank.

The Bank reserves the right to replace a Debit Card with a new one even during the period of validity of the Debit Card. The cardholder shall not incur any costs as a result.

When a new card is issued, the Bank will via Visa or Mastercard automatically update the relevant payment data (cardholder name, expiry date and card number) at merchants who also participate in the service. The cardholder can object to an automatic transmission of the card data by sending an e-mail to support@solarisbank.de.

16. Cardholder's right of termination

The cardholder may terminate the card contract at any time without any notice period.

17. Right of termination of the Bank

The Bank may terminate the card contract with an appropriate period of notice of at least two months. The Bank shall terminate the card contract with a longer notice period if this is necessary in view of the legitimate interests of the cardholder.
The Bank may terminate the card contract without notice if there is an important reason why continuation of the card contract is not reasonable for the Bank, even taking appropriate account of the legitimate interests of the cardholder.
Such a reason exists, in particular, if the cardholder has provided incorrect information about his financial situation and the Bank took the decision to conclude the card contract on that basis, or if a significant deterioration in his financial situation comes about or threatens to do so and, as a result, settlement of the obligations under the card contract in respect of the Bank is put at risk.

18. Consequences of termination

When termination comes into effect, the Debit Card may not be used further. The Debit Card shall be returned to the Bank immediately and without request. The cardholder shall arrange for additional company-generated applications on the Debit Card to be removed without delay by the company that set up the additional application on the Debit Card. The option to continue using a bank-generated additional application is governed by the regulations that apply to the additional application in question.

19. Revocation and blocking of the Card

(1) The Bank may block the Debit Card and revoke the Debit Card (at cash machines, for example)

- if it is entitled to terminate the card contract for good cause,
- if material grounds in connection with the security of the Debit Card justify it, or
- if there is a suspicion of unauthorised or fraudulent use of the Debit Card.

The Bank shall notify the cardholder of the block, specifying the relevant reasons, if possible before the block, but at the latest immediately after the block. The Bank shall unblock the Debit Card or replace it with a new Debit Card when the reasons for the block cease to obtain. The cardholder shall also receive immediate notification of this.
(2) If the Debit Card has a TAN generator or a signature function for online banking, blocking the Debit Card also results in blocking access to online banking.
(3) If the cardholder has saved an additional application on a revoked card, revocation of the Debit Card means that he can no longer use the additional application. The cardholder may demand from the Bank release of company-generated additional applications stored on the Debit Card at the time of its revocation, once the latter has received the Debit Card from the place at which it was revoked. The Bank is entitled to fulfil the demand for release of company-generated additional applications by providing the cardholder with the Debit Card with the payment functions removed from it. The option to continue using a bank-generated additional application on the Debit Card is governed by the regulations that apply to the additional application in question.

II. Additional applications

1. Saving additional applications on the Card

(1) The chip on the Debit Card can also be used as a storage medium for a bank-generated additional application (in the form of a feature for protection of minors, for example) or for a company-generated additional application (in the form of an electronic travel ticket, for example).
(2) The use of a bank-generated additional application is determined by the legal relationship of the cardholder to the card-issuing bank.
(3) The cardholder may use a company-generated additional application in accordance with the terms of the contract concluded with the company. The cardholder shall decide whether he wishes to use his Debit Card to save a company-generated additional application. A company-generated additional application is saved to the Debit Card at the company's terminal by agreement between the cardholder and the company. Financial institutions are not aware of the content of the data communicated at the company's terminal.

2. Responsibility of the company for the content of a company-generated additional application

The card-issuing bank only provides the technical platform, in the form of the chip, that allows the cardholder to save company-generated additional applications to the card. Any service that the company provides for the cardholder via the company-generated additional application is governed exclusively by the content of the contractual relationship between the cardholder and the company.

3. Processing of complaints with additional applications

(1) The cardholder shall pursue objections relating to the content of a company-generated additional application exclusively with the company that saved the additional application to the card. The company shall process such objections on the basis of the data stored with it. The cardholder may not hand over the Debit Card to the company for the purposes of processing the complaint.
(2) The cardholder shall pursue objections relating to the content of a bank-generated additional application exclusively with the Bank.

4. No information about the PIN issued to the cardholder by the Bank in company-generated additional applications

When saving, making changes to the content of or using a company-generated additional application on the card, the PIN issued to the cardholder by the card-issuing bank shall not be entered.
If the company that has saved a company-generated additional application to the Debit Card gives the cardholder the opportunity to secure access to this additional application with a separate legitimation medium selected by him, the cardholder may not use the PIN that has been given to him by the card-issuing bank for use of the payment transaction applications to safeguard the company-generated additional application.

5. Blocking options for additional applications

Blocking of a company-generated additional application can only be carried out by the company that saved the additional applica-

tion to the chip on the Debit Card and is possible only if the company has provided the option to block its additional application. Blocking of a bank-generated additional application can only be carried out by the Bank and is governed by the contract concluded with the Bank.

III. Changes to the Terms & Conditions of Business

Changes to these Terms & Conditions of Business shall be proposed to the cardholder by the Bank in written form no later than two months before they are to take effect. If the cardholder has agreed an electronic means of communication with the Bank as part of the business relationship (online banking, for example), the changes may also be proposed by this means. The cardholder is deemed to have consented if he fails to provide notice of his rejection in advance of the proposed date of the changes coming into effect. The Bank shall make specific reference to this de facto consent in its offer.

If the cardholder is notified of changes to these Terms & Conditions, he may cancel this business relationship without notice and at no cost in advance of the proposed date of the change coming into effect. The Bank shall make specific reference to this right to terminate in its offer.

IV. Out-of-court settlement of disputes and other possibilities of complaint

- The cardholder has the following out-of-court options:
  The cardholder may address a complaint to the point specified by the Bank in its "List of Prices and Services". The Bank will answer complaints in an appropriate manner; where payment service contracts are concerned, it will do so in text form (e.g. by letter, telefax or e-mail).
- In addition, the cardholder may make complaints at any time in writing or orally on the record to the German federal Financial Supervisory Authority [*Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin*], Graurheindorfer Straße 108, 53117 Bonn, about breaches by the Bank of the German Payment Services Supervision Act [*Zahlungsdiensteausichtsgesetz*], Sections 675c – 676c of the German Civil Code [*Bürgerliches Gesetzbuch*] or Article 248 of the Act Introducing the German Civil Code [*Einführungsgesetz zum Bürgerlichen Gesetzbuch*].
- - The European Commission has set up a European Online Dispute Resolution (ODR) Platform at http://ec.europa.eu/consumers/odr/. The Bank does not participate in dispute resolution proceedings with any consumer conciliation board.