Provisions on the Cardholder‘s Duty of Care

The ɎAPEAL debit card and notes on associated security-relevant data (e.g., PIN) must be kept separately from each other and protected from unauthorized access.

When ordering the debit card, a PIN must be defined for the card, which is known only to the cardholder. This PIN should not have any reference to the cardholder (e.g., telephone numbers, date of birth).

The cardholder must keep the PIN secret. He must not disclose it to any other person or make it accessible to others in any form. The PIN must always be entered in a concealed manner.

Likewise, the cardholder may not disclose the debit card or individual data relating to debit cards, in particular the card number and Card Validation Code, to other persons.

For certain Internet transactions, merchants require two-stage authentication. In this case, the transactions must be confirmed during the payment process by means of an SMS code (one-time password). The cardholder is obliged to check the transactions to be confirmed for correctness. Unknown or incorrect transactions must not be confirmed and SMS codes for two-step authentication must not be passed on to third parties.

Activation of a debit card for mobile payment may also require two-step authentication via SMS code (one-time password) or via the ɎAPEAL front-ends. The cardholder is obliged to check the activation to be confirmed for correctness. Unknown activations or activations not made by the cardholder may not be confirmed and SMS codes for two-step authentication may not be passed on to third parties.

The Cardholder must act in good faith and take due care of the debit cards and devices activated for Mobile Payment. Under no circumstances may the cardholder allow another person to use them. This includes protecting the devices securely from access by third parties (device-dependent: e.g., secure PIN, biometric login).

If the cardholder notices or suspects that the terminal device or digital debit card or individual information has come into the control of an unauthorized person (in particular loss or theft) or that unauthorized transactions have been made via it, the cardholder is obligated to immediately change access features and methods and/or have the mobile payment function blocked immediately via the respective provider and to inform Urban Connect without delay.

If these GTCs are available in translation, only the German-language version is binding.

Sorgfaltspflichten von Karteninhabern

Die YAPEAL Debitkarte und Notizen zu dazugehörigen sicherheitsrelevanten Daten (beispielsweise PIN) sind getrennt voneinander und vor Fremdzugriffen geschützt aufzubewahren.

Bei der Bestellung der Debitkarte muss eine PIN für die Karte definiert werden, welche nur dem Karteninhaber selbst bekannt ist. Diese PIN sollte keinen Bezug zum Karteninhaber haben (z.B. Telefonnummern, Geburtsdatum).

Der Karteninhaber muss die PIN geheim halten. Er darf sie keinen anderen Personen bekannt geben oder in irgendeiner Form für andere zugänglich machen. Die Eingabe der PIN muss stets verdeckt erfolgen.

Ebenso darf der Karteninhaber die Debitkarte sowie Debitkarten betreffende einzelne Daten, insbesondere die Kartennummer und Prüfziffer, nicht an andere Personen weitergeben.

Für bestimmte Internet-Transaktionen wird von Händlern eine zweistufige Authentifizierung gefordert. Die Transaktionen müssen in diesem Fall beim Bezahlvorgang mittels SMS-Code (Einmalpasswort) bestätigt werden. Der Karteninhaber ist verpflichtet, die zu bestätigenden Transaktionen auf Ihre Korrektheit zu prüfen. Unbekannte oder nicht korrekte Transaktionen dürfen nicht bestätigt und SMS-Codes für die zweistufige Authentifizierung nicht an Dritte weitergegeben werden.

Auch die Aktivierung einer Debitkarte für Mobile Payment bedingt möglicherweise eine zweistufige Authentifizierung mittels SMS-Code (Einmalpasswort) oder über die YAPEAL-Frontends. Der Karteninhaber ist verpflichtet, die zu bestätigenden Aktivierung auf Ihre Korrektheit zu prüfen. Unbekannte bzw. nicht durch ihn getätigte Aktivierungen dürfen nicht bestätigt und SMS-Codes für die zweistufige Authentifizierung nicht an Dritte weitergegeben werden.

Der Karteninhaber muss im guten Glauben handeln und die für Mobile Payment aktivierten Debitkarten und Endgeräte mit der gebotenen Sorgfalt verwahren. Der Karteninhaber darf unter keinen Umständen zulassen, dass eine andere Person diese verwenden kann. Dies beinhaltet, die Endgeräte sicher vor dem Zugriff Dritter zu schützen (geräteabhängig: sicherer PIN, biometrischer Login, etc.).

Wenn der Karteninhaber bemerkt oder den Verdacht hegt, dass das Endgerät oder die digitale Debitkarte bzw. einzelne Informationen in den Besitz oder unter die Kontrolle einer nicht autorisierten Person gelangt ist (insbesondere Verlust oder Diebstahl) oder dass darüber nicht autorisierte Transaktionen getätigt wurden, ist er dazu verpflichtet, Zugangsmerkmale und -methoden sofort zu ändern und/oder die mobile Bezahlfunktion über den jeweiligen Anbieter sofort sperren zu lassen und Urban Connect unverzüglich zu informieren.

Ungeachtet von Übersetzungen dieser AGB, ist die Version in deutscher Sprache verbindlich.

Urban Connect