

## Merkblatt „Informationen über Internetzahlungen“

---

### Bezahlen im Internet/sicheres Verfahren

Als Karteninhaber erhalten Sie per Post die von Ihnen beantragte(n) Mastercard und/oder Visa Karte(n) (Debit- oder Kreditkarte (n)) – nachfolgend kurz „Karte“ genannt – und mit getrennter Post die persönliche Geheimzahl (PIN) für Transaktionen an Kartenzahlungsterminals und an Geldautomaten. Die Karte kann, wie in Ziffer 4.3 der „Vertragsbedingungen für Mastercard und Visa Karten“ (nachfolgend kurz „Vertragsbedingungen“) beschrieben, für Zahlungen im Internet verwendet werden.

Durch Ihren Kartenantrag bestätigen Sie, dass Sie über diese Möglichkeit zur Internetzahlung informiert sind und diese akzeptieren bzw. wünschen. Als Karteninhaber haben Sie darauf zu achten, dass die übermittelten Kartendaten verschlüsselt („<https://>“) übertragen werden (vgl. Ziffer 6.4 der Vertragsbedingungen). Bitte setzen Sie die Karte im Internet nur in einer sicheren Umgebung ein (Details siehe nachfolgend unter „Sicherer Karteneinsatz im E-Commerce“). Die Eingabe Ihrer Kartendaten über unverschlüsselte Verbindungen, die Preisgabe Ihrer Kartendaten aufgrund von E-Mail-Anforderungen (z. B. angebliche Sicherheitsüberprüfungen, nicht angeforderte Benutzerkonto-Entsperrungen o. Ä.) oder die Freigabe anderer Geldbeträge oder Empfänger als erwartet bergen Risiken für sichere Zahlungen. Die Gefahr besteht insbesondere darin, dass Unberechtigte Ihre Kartendaten einschließlich der Autorisierungsdaten ausspähen und für unberechtigte Transaktionen einsetzen können.

Sofern von der Akzeptanzstelle das Kundenauthentifizierungsverfahren Mastercard Identity Check™/Visa Secure (im Folgenden „sicheres Bezahlfahrer“) unterstützt und dessen Nutzung durch den Herausgeber gefordert wird, ist dieses von Ihnen als Karteninhaber einzusetzen (vgl. Ziffer 4.3 der Vertragsbedingungen). Bitte registrieren Sie sich daher direkt nach Erhalt Ihrer Karte auf unserer Internetseite für das entsprechende sichere Bezahlfahrer.

Stellen Sie sicher, dass kein Anderer Kenntnis von den Kennungen für dieses Bezahlfahrer erlangt (vgl. Ziffer 6.4 der Vertragsbedingungen).

### Schritt für Schritt Anleitung des Registrierungsvorgangs

Eine gesonderte Beschreibung des Anmelde- und Registrierungsvorgangs stellen wir Ihnen getrennt zur Verfügung.

**Der Zahlungsrahmen**, der Ihnen mit Übersendung der Karte erstmalig mitgeteilt wird und in Abstimmung mit der Bank geändert werden kann, **gilt sowohl für das persönliche Bezahlen in der Akzeptanzstelle wie auch für das Bezahlen im Internet**. Die Internetzahlungsfunktion lässt sich auf Ihren Wunsch in der monatlichen Höhe begrenzen oder deaktivieren.

### Sicherer Karteneinsatz im E-Commerce

#### Information über die Mindestanforderungen an die Sicherheit von Internetzahlungen

Sie können mit Ihrer Karte im Internet Waren und Dienstleistungen bezahlen. Gemäß Ziffer 4.3 der Vertragsbedingungen dürfen bei einer Kartenzahlung im Internet nur folgende Daten angegeben werden:

- Ihr Name,
- die Kartenmarke (Mastercard/Visa),
- die Kartenummer,
- das Laufzeitende der Karte und
- die auf der Kartenrückseite genannte dreistellige Kartenprüfziffer

Bitte geben Sie niemals die PIN an, die Sie für Zahlungen an Kartenzahlungsterminals oder zur Bargeldauszahlung am Geldautomaten erhalten haben! Eine auf Ihrem Mobiltelefon erhaltene E-Commerce-TAN zur Authentifizierung der Zahlung darf nur eingegeben werden, wenn Zahlungsempfänger, Betrag und Währung geprüft wurden und mit der freizugebenden Zahlung übereinstimmen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt auf seinen Internetseiten (<https://www.bsi-fuer-buerger.de>) die nachfolgenden 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet:

1. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte Sicherheitsupdates für Ihr Betriebssystem und die von Ihnen installierten Programme – idealerweise über die Funktion „Automatische Updates“.
2. Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig.
3. Verwenden Sie eine Personal Firewall.
4. Nutzen Sie für den Zugriff auf das Internet ausschließlich ein Benutzerkonto mit eingeschränkten Rechten, keinesfalls ein Administrator-Konto.
5. Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch. Klicken Sie nicht automatisch auf jeden Link oder jeden Dateianhang, der Ihnen per E-Mail gesendet wird.
6. Verwenden Sie einen modernen Internet-Browser mit fortschrittlichen Sicherheitsmechanismen.
7. Nutzen Sie möglichst sichere Passwörter. Verwenden Sie für jeden genutzten Online-Dienst ein anderes sicheres Passwort. Ändern Sie diese Passwörter regelmäßig. Vom Anbieter oder Hersteller voreingestellte Passwörter sollten Sie sofort ändern.
8. Wenn Sie im Internet persönliche Daten übertragen wollen, nutzen Sie ausschließlich eine verschlüsselte Verbindung (zu erkennen an: „<https://>“).
9. Deinstallieren Sie nicht benötigte Programme.
10. Erstellen Sie regelmäßig Sicherheitskopien („Backups“) Ihrer Daten.
11. Wenn Sie ein WLAN („Wireless LAN“, drahtloses Netzwerk) nutzen, sollte dies stets mittels des Verschlüsselungsstandards WPA2 verschlüsselt sein.
12. Überprüfen Sie in regelmäßigen Abständen den Sicherheitsstatus Ihres Computers.

Berücksichtigen Sie die erheblichen Bedrohungen und Risiken, die mit dem Herunterladen von Software über das Internet verbunden sind, wenn Sie nicht mit hinreichender Sicherheit feststellen können, ob die Software echt ist und nicht manipuliert wurde.

Sofern Sie den Verdacht haben, dass Ihre Kartendaten auf Ihrem Computer ausgespäht wurden, sperren Sie Ihre Karte sofort telefonisch unter der auf dem Übersendungsschreiben, der Kartenrückseite und der Umsatzaufstellung mitgeteilten 24-Stunden-Rufnummer (Sperrannahme-Service) +49 (0) 721 1209-66001. Lassen Sie Ihre Karte auch unverzüglich sperren, wenn Sie den Verlust der Karte oder missbräuchliche Nutzung der Karte, der Kartendaten oder eines Legitimationsmediums feststellen oder einen entsprechenden Verdacht haben (vgl. Ziffer 6.5 der Vertragsbedingungen). Sofern Sie auf Ihrem mobilen Endgerät eine digitale Karte nutzen und Ihnen das Gerät abhandengekommen ist, sperren Sie diese digitale Karte sofort telefonisch unter der vorstehenden Sperr-Rufnummer.

Informationen zur Beseitigung von Schadsoftware auf Ihrem Computer finden Sie ebenfalls im Internetauftritt des BSI in der Informationstechnik unter dem Stichwort „Risiken/Schadprogramme/Infektionsbeseitigung“.

Sie können sich jederzeit auf der Internetseite des BSI unter „Service/Aktuell“ über aktuelle Sicherheitswarnungen und Sicherheitsupdates informieren.

#### **Information über Umsatzausführung**

Im Online-Banking bzw. der von Ihrer Bank bereitgestellten Banking-App haben Sie jederzeit die Möglichkeit, die gebuchten Umsätze und den Saldo Ihrer Karte einzusehen.

#### **Information und Kontaktaufnahme im Fall von Missbrauchsverdacht oder neuen Sicherheitsmaßnahmen**

Ihre Karte ist ein sicheres Zahlungsmittel. Vor Betrug schützen Sie auch Präventions- und Monitoringsysteme, die versuchen, Auffälligkeiten beim Karteneinsatz, frühzeitig vor dem Hintergrund allgemeiner Erfahrungswerte, aktueller Vorfälle und auch anhand Ihres bisherigen Karteneinsatzes zu entdecken. Es kann daher in Einzelfällen vorkommen, dass eine beabsichtigte Transaktion einer Überprüfung bedarf oder nicht ausgeführt wird. Wir werden Sie bei sicherheitsrelevanten Vorfällen telefonisch, per Brief, über eine Mitteilung auf dem Kontoauszug oder, sofern Sie dieses nutzen, über das elektronische Postfach in Ihrem Online-Banking bzw. der von Ihrer Bank bereitgestellten Banking-App informieren. Informationen zu allgemeinen Sicherheitsmaßnahmen (z. B. Warnung vor Phishing-E-Mails) erhalten Sie auch auf der Internetseite Ihrer Bank.

Ebenso können Sie Auffälligkeiten, Unregelmäßigkeiten während der Sitzung bei Internetzahlungsdiensten, unerwartete Aufforderungen zur Preisgabe von Karten- oder Legitimationsdaten oder einen Missbrauchsverdacht jederzeit über die Sperr-Hotline +49 (0) 721 1209-66001 telefonisch melden. Je nach Ergebnis der Abstimmung mit Ihnen kann Ihre Karte wieder eingesetzt und der Zahlungsauftrag ausgeführt werden oder bei Verdacht auf Missbrauch wird die Karte gesperrt und kostenfrei ersetzt.

#### **Beschreibung der Haftung**

Sofern der Karteninhaber einen Zahlungsauftrag nicht autorisiert hat, nicht vorsätzlich oder missbräuchlich gehandelt hat und alle Sorgfaltspflichten laut Vertragsbedingungen eingehalten hat, haftet er nicht für die nicht autorisierten Umsätze. Andernfalls richtet sich die Haftung nach den in den Vertragsbedingungen beschriebenen Regelungen.