Bestellung Zugangsdaten
für das Smart Data Portal
zur PayLife Business Karte

Ihr Servicekontakt:
PayLife Service Center | Wiedner Gürtel 11 | 1100 Wien
+43 (0)5 99 06-2900 | kartenservice@paylife.at
www.paylife.at

Bitte in Blockschrift ausfüllen und an das PayLife Service Center per E-Mail zusenden!

Zugangsdaten Smart Data Version 1 07/2023

1 Angaben zur Firma

Firmenwortlaut | Firmentelefonnummer

Straße, Hausnummer | PLZ, Ort, Land

Der Zugang zu PayLife Smart Data ist kostenlos. Dem Karteninhaber steht außerdem das kostenlose Serviceportal my.paylife.at zur Verfügung. Weitere Informationen finden Sie unter www.paylife.at/onlineservices.

2 Daten des Company Programm Administrator

Der Company Pogramm Administrator (CPA) tritt als Ansprechperson und Verantwortlicher für die Firma bezüglich PayLife Smart Data gegenüber BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) auf. Der CPA hat alle umfassenden Lese und Schreibrechte.

☐ Frau ☐ Herr | Titel | Geburtsdatum (TT/MM/JJJJ)

Vorname | Nachname | Position im Unternehmen

E-Mail-Adresse (bis zu 40 Zeichen) | Telefonnummer (für Rückfragen)

PayLife Kundenkontonummer (auf der Abrechnung ersichtlich)

3 Firmenmäßige Fertigung

Hinweis: Nur bei Zustimmung beider Checkboxen, kann ein Zugang ausgestellt werden.

☐ Ich erkläre hiermit, dass die Besonderen Geschäftsbedingungen für das "Smart Data" Portal vereinbart werden.

☐ Ich erkläre hiermit, dass Name, Kartennummer, Transaktionsdaten, Ablaufdatum der Karte, Adresse, Telefonnummer und Email-Adresse zur Abwicklung des SmartData Vertrages an Mastercard International Incorporated, 2000 Purchase Street, Purchase, New York 10577, USA übermittelt werden. Grundlage für die Übermittlung der Daten in die USA sind die Binding Corporate Rules von Mastercard (mastercard-bcrs.pdf), die datenschutzrechtliche Regelungen enthalten. Den USA wird vom Europäischen Gerichtshof kein angemessenes Datenschutzniveau bescheinigt. Es besteht insbesondere das Risiko, dass die Daten dem Zugriff durch US-Behörden zu Kontroll- und Überwachungszwecken unterliegen und dagegen keine wirksamen Rechtsbehelfe zur Verfügung stehen. Die Zustimmung kann jederzeit mit Wirkung für die Zukunft widerrufen werden (kartenservice@paylife.at). Weitere Datenschutzinformationen finden sie unter www.paylife.at/datenschutz .

Wegen Beschwerden und der Durchsetzung der Binding Corporate Rules von Mastercard wenden Sie sich an:
– BindingCorporateRules@mastercard.com unter Angabe des Begriffs „BCRs" in der Betreffzeile; oder
– Mastercard Europe SA, Privacy & Data Protection Team, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgien.

Ort, Datum

X
Firmenstempel und Unterschrift des handlungsbefugten Organs oder Bevollmächtigen

Besondere Geschäftsbedingungen für das „Smart Data“ Portal

Diese Besonderen Geschäftsbedingungen sind aus Gründen der leichteren Lesbarkeit nicht geschlechterspezifisch formuliert und gelten in gleicher Weise für alle Geschlechter

1. Allgemeines

1.1. Diese Besonderen Geschäftsbedingungen für das Smart Data Portal (kurz: BGB Smart Data) regeln das Online Service von Mastercard International Incorporated, 2000 Purchase Street, Purchase, New York 10577, USA (Kurz: Mastercard) zu den von der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) ausgegebenen PayLife Firmenkreditkarten (kurz: Karte) in Österreich und Deutschland und regeln die Nutzung dieses Services durch den Company Programm Administrator (kurz: CPA), welcher als Ansprechperson und Verantwortlicher für das Unternehmen bezüglich Smart Data auftritt. Die BGB Smart Data gelten, wenn sie mit dem Unternehmen vereinbart sind. Die BGB gelten ergänzend zu den zwischen der Bank und dem Unternehmen vereinbarten Allgemeinen Geschäftsbedingungen für PayLife Firmenkreditkarten (kurz: AGB).

1.2. Mastercard ist Eigentümer und Betreiber des Systems Smart Data.

1.3. Die Möglichkeit zur Nutzung von Smart Data setzt einen gültigen Kreditkartenvertrag über eine PayLife Firmenkreditkarte (kurz: Kartenvertrag) zwischen der Bank und dem Unternehmen und den Abschluss einer Vereinbarung über die Nutzung des Smart Data Portals durch das Unternehmen voraus.

1.4. Um das Smart Data Portal nutzen zu können, muss sich das Unternehmen auf der Website smartdata.paylife.at registrieren.

2. Smart Data Portal

2.1. Das Smart Data genannte Portal der Mastercard ermöglicht dem CPA, Informationen zu der Paylife Firmenkreditkarte einzusehen, Abfragen (insbesondere Umsatzabfragen) zu tätigen und die Online Abrechnung (= Sammelabrechnung) herunterzuladen. Im Rahmen des Smart Data Portals können keine Zahlungsaufträge und rechtsverbindliche Willenserklärungen erteilt werden; auch eine Verwendung der Karte ist nicht möglich.

2.2. Es ist die alleinige Verantwortung des Unternehmens, auf eigene Kosten Betriebssysteme, Software, Hardware oder Dienstleistungen zu beschaffen und zu warten, die für den Zugang zu Smart Data und dessen Nutzung durch autorisierte Nutzer des Unternehmens erforderlich sind.

2.3. Das Unternehmen muss den Zugriff zum Portal per Formular beantragen. Das Unternehmen kann dies jederzeit beauftragen.

2.4 Das Unternehmen ist verpflichtet, den Zugang zu Smart Data und der Dokumentation auf seine autorisierten Mitarbeiter zu beschränken.

2.5. Ist zwischen der Bank und dem Unternehmen vereinbart, dass die Bank die Online Abrechnung (= Sammelabrechnung) zu den PayLife Firmenkreditkarten dem Unternehmen online zum Download zur Verfügung stellt, erfolgt dies im Rahmen des Smart Data Portals.

2.6 Smart Data steht via Internet Browser auf der Website smartdata.paylife.at zur Verfügung.

3. Definitionen und Begriffsbestimmungen

3.1 Benutzer-ID (kurz: Benutzer-ID)
Der CPA erhält als Identifikationsmerkmal eine mehrstellige Benutzer-ID, welche von ihm nicht geändert werden kann. Die Benutzer-ID dient sowohl bei der Registrierung als auch bei der Anmeldung des CPA zum Smart Data Portal als Identifikationsmerkmal.

3.2 Einmalpasswort
Das Einmalpasswort ist ein von der Mastercard vorgegebenes Identifikationsmerkmal, das vom CPA nicht geändert werden kann; es dient der Legitimierung des CPA bei der Registrierung im Smart Data Portal.

3.3. Passwort (kurz: Kennwort)
Das Passwort ist das vom CPA bei der Registrierung zum Smart Data Portal festgelegte Geheimwort (Kombination aus Zeichen). Das Passwort ist ein persönliches Identifikationsmerkmal des CPA, welches bei zusätzlicher Angabe der Benutzer-ID der Identifizierung des CPA für den Zugang zum Smart Data Portal dient. Das Passwort kann vom CPA im Smart Data Portal geändert werden.

3.4. Die Sicherheitsfrage/-antwort
Die Sicherheitsfrage und Sicherheitsantwort ist vom CPA bei der Registrierung zum Smart Data Portal festgelegt worden. Die Sicherheitsfrage und Sicherheitsantwort ist ein persönliches Identifikationsmerkmal des CPA, welches bei zusätzlicher Angabe der Benutzer-ID der Identifizierung des CPA für das Zurücksetzen des Passworts im Smart Data Portal dient. Die Sicherheitsfrage und Sicherheitsantwort kann vom CPA im Smart Data Portal geändert werden.

4. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen

Das Unternehmen ist verpflichtet, den Zugang zum System und der Dokumentation auf seine autorisierten Mitarbeiter zu beschränken. Alle Handlungen der autorisierten Mitarbeiter im Zusammenhang mit dem Smart Data Portal werden dem CPA direkt zugerechnet. Der CPA und das Unternehmen sind zur Einhaltung der nachstehenden vereinbarten Sorgfaltspflichten verpflichtet.

4.1. Geheimhaltungs- und Sperrverpflichtung

(1) Der CPA und das Unternehmen haben die persönlichen Identifikationsmerkmale (Passwort, Einmalpasswort, Benutzer-ID, Sicherheitsfrage/-antwort) geheim zu halten; sie dürfen Dritten nicht mitteilen oder in einer sonstigen Form offenlegen.

(2) Der CPA und das Unternehmen sind verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung der Identifikationsmerkmale walten zu lassen, um einen missbräuchlichen Zugriff auf das Smart Data Portal zu vermeiden. Es ist insbesondere darauf zu achten, dass bei Verwendung der persönlichen Identifikationsmerkmale diese nicht ausgespäht werden können. Sie dürfen weder auf dem Gerät, von dem aus in das Smart Data Portal eingestiegen wird, noch im Endgerät, in welches Identifikationsmerkmale zugestellt werden, notiert bzw. gespeichert werden (etwa in einer App für Notizen).

(3) Bei Verlust oder Diebstahl von persönlichen Identifikationsmerkmalen sowie dann, wenn das Unternehmen oder der CPA von einer missbräuchlichen oder einer sonstigen nicht autorisierten Nutzung des Smart Data Portals Kenntnis erlangt haben, haben der CPA oder das Unternehmen unverzüglich die Sperre des Zugangs zum Smart Data Portals zu veranlassen.

4.2. Empfohlene Sicherheitsmaßnahmen bei der Nutzung des Smart Data Portals

(1) Dem CPA wird empfohlen, das gewählte Passwort regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.

(2) Dem CPA wird empfohlen, bei Verlust oder Diebstahl des Endgeräts, auf welches er Identifikationsmerkmale erhält, unverzüglich das Passwort zu ändern oder die Sperre des Zugangs zu Smart Data zu veranlassen.

(3) Dem CPA und dem Unternehmen werden empfohlen, unverzüglich das Passwort zu ändern oder die Sperre des Zugangs zu Smart Data zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von den persönlichen Identifikationsmerkmalen haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten den Missbrauch ermöglichen könnten.

5. Sperre

5.1. Der Zugang zu Smart Data wird gesperrt, wenn während eines Zugriffs sechs Mal aufeinanderfolgend das Passwort falsch eingegeben wird. Ebenfalls wird der Zugang gesperrt, wenn der CPA sich nicht innerhalb von 90 Tagen mindestens einmal in Smart Data eingeloggt hat.

5.2. Die Aufhebung einer Sperre ist durch den CPA per E-Mail an kartenservice@paylife.at oder durch den Kennwort/Pin vergessen?- Prozess in Smart Data möglich.

5.3. Der CPA und das Unternehmen kann die permanente Sperre des Zuganges zum Smart Data Portal per E-Mail unter kartenservice@paylife.at veranlassen.

5.4. Die Bank ist berechtigt, Smart Data zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen, oder der Verdacht einer nicht autorisierten oder betrügerischen

Verwendung besteht. Die Bank wird eine Sperre aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen oder der CPA die Aufhebung der Sperre beauftragt.

6. Vertragsdauer, Kündigung und Beendigung

6.1. Die Vereinbarung über die Teilnahme an Smart Data wird auf unbestimmte Zeit geschlossen. Die Vereinbarung über die Teilnahme an Smart Data endet jedoch automatisch sobald kein aufrechter Kartenvertrag des Unternehmens mit der Bank besteht.

6.2. Der CPA und das Unternehmen sind berechtigt, die Vereinbarung über die Teilnahme an Smart Data jederzeit ohne Angabe von Gründen und ohne Kündigungsfrist zu kündigen. Nach Einlangen der Kündigung wird die Bank den Zugriff auf Smart Data sperren.

6.3. Die Bank ist berechtigt, die Vereinbarung über die Teilnahme an Smart Data jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen.

6.4. Sowohl das Unternehmen als auch die Bank sind berechtigt, die Vereinbarung über die Teilnahme an Smart Data jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen.

6.5. Die Beendigung der Vereinbarung über die Teilnahme an Smart Data lässt den Kartenvertrag unberührt, falls das Unternehmen bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.

7. Änderungen der BGB Smart Data

7.1. Änderungen dieser BGB und des Leistungsumfangs im Zusammenhang mit Smart Data werden dem Unternehmen durch Übermittlung der Information per E-Mail oder per Post zur Kenntnis gebracht. Sollten der Bank divergierende (E-Mail-)Adressen vom CPA und dem Unternehmen mitgeteilt werden, erfolgen Zustellungen an die zuletzt bekannt gegebene (E-Mail-)Adresse. Die Änderungen der Besonderen Geschäftsbedingungen und des Leistungsumfangs gelten als genehmigt und vereinbart, wenn der CPA oder das Unternehmen nicht innerhalb von 2 Monaten nach Zustellung widerspricht.

8. Haftungsausschluss

8.1. Weder Mastercard noch die Bank übernehmen eine Gewährleistung in Bezug auf die Verlässlichkeit, Richtigkeit oder Vollständigkeit der im Portal enthaltenen Informationen.

Fassung Juli 2023

Ergänzung zum "Informationsblatt zum Datenschutz für in Österreich ausgegebene Kreditkarten und nicht anonyme Prepaid Karten" bei Nutzung von dem Portal "Smart Data"

5. Werden Daten an ein Drittland oder an eine internationale Organisation übermittelt?

Smart Data von Mastercard
Wenn Sie das Firmenkundenprodukt SmartData nutzen, werden Name, Kartennummer, Transaktionsdaten, Ablaufdatum der Karte, Adresse, Telefonnummer, Email und IP-Adresse zur Abwicklung Ihres Vertrages an Mastercard International Incorporated, 2000 Purchase Street, Purchase, New York 10577, USA übermittelt. Grundlage für die Übermittlung der Daten in die USA sind die Bin-ding Corporate Rules von Mastercard (mastercard-bcrs.pdf), die datenschutzrechtliche Regelungen enthalten.

7. Welche Datenschutzrechte stehen mir zu?

Sie haben jederzeit ein Recht auf Auskunft, Berichtigung, Lö-schung oder Einschränkung der Verarbeitung Ihrer gespeicherten Daten, ein Widerspruchsrecht gegen die Verarbeitung sowie ein Recht auf Datenübertragbarkeit gemäß den Voraussetzungen des Datenschutzrechts. Beschwerden können sie an die Österreichi-sche Datenschutzbehörde unter dsb@dsb.gv.at richten.

Smart Data von Mastercard
Wegen Beschwerden und der Durchsetzung der Binding Corporate Rules von Mastercard wenden Sie sich an:
BindingCorporateRules@mastercard.com unter Angabe des Begriffs "BCRs" in der Betreffzeile; oder
Mastercard Europe SA, Privacy & Data Protection Team, Chaus-sée de Tervuren 198A, B-1410 Waterloo, Belgien.

Stand Juli 2023