Mobiles Bezahlen
Datenschutzerklärung

Version: 12/2020

Diese Datenschutzerklärung informiert Sie (im Folgenden „**Nutzer**“, „**Sie**“, „**Ihnen**“) über die Verarbeitung Ihrer personenbezogenen Daten bei der Nutzung der Mobile App „Mobiles Bezahlen“ (die „**App**“) mit Einsatz von digitalen Zahlungskarten.

1. Allgemeines

Die S-Payment GmbH, Am Wallgraben 115, 70565 Stuttgart (im Folgenden „**S-Payment**“) bietet die App für die Nutzung auf mobilen Endgeräten mit Android-Betriebssystemen an. Weitere Informationen zur App finden Sie z. B. in den Lizenz- und Nutzungsbedingungen zu der App.

In der App können Nutzer digitale Versionen ihrer bereits vorhandenen physischen Zahlungskarten (wie girocards oder Kreditkarten), wie sie ihnen von ihrer Bank oder Sparkasse (zusammen „**Institute**“) nach Maßgabe der Kartenbedingungen, Nutzungshinweise und -voraussetzungen des Instituts angeboten werden (die „**digitale Karte**“), auf Basis der sog. HCE-Technologie (Host Card Emulation) in einer Art digitalen Brieftasche hinterlegen, um an POS-Kassensystemen von Unternehmen, die diese digitalen Karten akzeptieren („**Akzeptanzstellen**“), mit ihren mobilen Endgeräten (Smartphone, Tablet) zu bezahlen.

Die App dient ausschließlich als digitales Aufbewahrungsmittel für die entsprechenden, vom Nutzer hinterlegten digitalen Karten (entsprechend einer Geldbörse bei physischen Zahlungskarten). S-Payment ist mit Blick auf die Integration der digitalen Karten in die App und die Unterstützung entsprechender Zahlungsvorgänge mittels der digitalen Karte des Instituts lediglich technischer Dienstleister bzw. Auftragsverarbeiter des Instituts und hat insbesondere keine Kontrolle über die auf den hinterlegten digitalen Karten enthaltenen Informationen bzw. die durch die Nutzer auf Basis der digitalen Karten ausgeführten Transaktionen.

Ausschließlich das Institut, das die digitale Karte herausgibt, erbringt die Zahlungsdienstleistung der Kartenzahlung. S-Payment erbringt gegenüber dem Nutzer keine Zahlungsdienstleistungen und ist von ihm auch nicht zur Ausführung, Auslösung oder Abwicklung von Zahlungen beauftragt.

In diesem Dokument finden Sie insbesondere Informationen dazu, welche Ihrer personenbezogenen Daten bei der Nutzung der App verarbeitet werden, wie diese Daten verarbeitet werden und welche Rechte Ihnen in diesem Zusammenhang zustehen.

2. Datenschutzrechtlich Verantwortliche

Datenschutzrechtlich Verantwortliche für die im Zusammenhang mit der App und dem Einsatz der vom Nutzer hinterlegten digitalen Karten verarbeiteten personenbezogenen

Daten sind je nach Verarbeitungsvorgang entweder S-Payment oder das Institut (welches Sie in der App über die Eingabe der entsprechenden Bankleitzahl ausgewählt haben; siehe dazu unten Ziffer 3.a); für weitere Informationen betreffend die Institute siehe auch Ziffer 7.b)). Die S-Payment ist verantwortlich für Datenverarbeitungen im Zusammenhang mit der Nutzung der App, die nicht in unmittelbarem Zusammenhang mit digitalen Karte stehen. Die Kontaktdaten des Datenschutzbeauftragten der S-Payment finden Sie unter Ziffer 7.a)).

Insofern die Verarbeitungsvorgänge im Rahmen der Abwicklung von Kartenzahlungen oder der Ausgabe (Provisionierung) von digitalen Karten erfolgen, ist das Institut verantwortlich. Entsprechende Auftragsverarbeitungsverträge zwischen Institut und S-Payment wurden abgeschlossen. Den wesentlichen Inhalt der entsprechenden Vereinbarungen zur Verarbeitung von Daten, die Ihr kartenausgebendes Institut betreffen, stellt Ihnen Ihr Institut auf Anforderung zur Verfügung (siehe zu den Kontaktdaten des entsprechenden Datenschutzbeauftragten Ziffer 7.b) unten).

3. Verarbeitung Ihrer Daten

a) Damit Sie die App nutzen können, müssen Sie zunächst bei der ersten Verwendung der App den Lizenz- und Nutzungsbedingungen der App zustimmen. Ihre Zustimmung wird von S-Payment in einem Logfile gespeichert.

Darüber hinaus ist es für eine Integration von digitalen Karten in der App erforderlich, dass Sie die Bankleitzahl Ihres Instituts in der App eingeben, damit die App eine Verbindung mit Ihrem Institut herstellen kann. Die Bankleitzahl wird zu diesem Zweck gespeichert.

Für die in Ziffer 3. a) genannten Verarbeitungsvorgänge ist die S-Payment verantwortliche Stelle.

b) Für die im Folgenden unter dieser Ziffer 3. b) dargestellten Verarbeitungsvorgänge (einschl. Übermittlungen an Dritte) ist Ihr kartenausgebendes Institut bzw. die jeweilige Akzeptanzstelle verantwortliche Stelle; soweit die S-Payment in diesem Zusammenhang Daten verarbeitet, handelt sie dabei lediglich als technischer Dienstleister des entsprechenden Instituts.

aa) Um eine digitale Karte zur Nutzung in der App abzurufen, müssen Sie nach der Eingabe der Bankleitzahl in einem weiteren Schritt über die allgemeine Onlinebanking-Schnittstelle zu Ihrem Institut die Onlinebanking-Zugangsdaten Ihres Instituts (Benutzername, Passwort) angeben. Diese Daten werden nicht durch S-Payment, sondern durch Ihr Institut in gleicher Weise wie bei einem allgemeinen Zugriff auf Ihre Onlinebanking-Anwendung verarbeitet.

bb) Nach der Eingabe der Onlinebanking-Zugangsdaten wird dem Nutzer eine Auswahl von Karten in der App angezeigt, die der Nutzer als digitale Karten zur Nutzung in der App aktivieren kann. Der Nutzer kann eine oder mehrere dieser digitalen Karten nach Maßgabe der Nutzungsvoraussetzungen und Hinweise seines Instituts auswählen. Wenn er eine digitale Karte auswählt, werden die physisch sichtbaren Kartendaten (Kartennummer, Ablaufdatum) mit der digitalen Karte sowie die zum Einsatz der digitalen Karte herunterzuladenden Einmalschlüssel in der App hinterlegt, damit die digitalen Karten für Zahlungseinsätze verwendet werden können.

cc) Bestimmte von den Instituten ausgegebene physische Karten (zurzeit Kreditkarten von Mastercard und Visa) können aus Sicherheitsgründen nach den Vorgaben der Kartensysteme nur in einem bestimmten territorialen Bereich auch als digitale Karte abgerufen werden. Ggf. wird im Zusammenhang mit der Auswahl von solchen Karten (vgl. zum Auswahlvorgang Ziffer 3. b) bb)) daher für Ihr Institut einmalig der Standort des Nutzers anhand von GPS-Daten ermittelt, um sicherzustellen, dass der Nutzer, der diese Karten aktivieren möchte, sich nicht in Ländern befindet, in denen die im Zusammenhang mit der App angebotenen digitalen Karten nicht ausgewählt werden können. Diese Standortdaten werden zu dem vorgenannten Zweck zusammen mit der dazugehörigen Kreditkartennummer des Nutzers an das entsprechende Kreditkartenunternehmen (wie z. B. Mastercard) weitergeleitet.

In der App wird bestimmte Root Detection-Technologie verwendet, um die App und Ihre Daten vor der missbräuchlichen Erweiterung von Schreib- und Leserechten durch den Nutzer selbst bzw. durch Dritte zu schützen. Bei einer Root Detection-Prüfung handelt es sich um eine lokal in der App vorgenommene Prüfung zu der Frage, ob für das entsprechende Endgerät erweiterte Schreib- und Leserechte (Rooting) eingeräumt wurden. In diesem Zusammenhang werden von S-Payment und Ihrem Institut grds. keine personenbezogenen Daten verarbeitet. Es wird in diesem Zusammenhang aber aus Missbrauchs- und Betrugsbekämpfungszwecken im Fall eines erkannten Rootings die Information in der App verarbeitet, dass ein entsprechendes Rooting stattgefunden hat. Zudem wird das Ergebnis der Rooting-Prüfung zu Missbrauchs- und Betrugsbekämpfungszwecken ggf. an die relevanten Kreditunternehmen übermittelt (zurzeit betrifft dies VISA).

Bei diesen Kreditkartenunternehmen handelt es sich zum Teil um Unternehmen mit Sitz in der EU sowie mit einem Hauptsitz in den USA (zurzeit Mastercard und VISA). Die vorstehend in Ziffer 3. b) cc) genannten Daten und ggf. auch weitere Daten betreffend die Abwicklung einer Zahlung werden von den entsprechenden Kreditkartenunternehmen (zu den vorgenannten bzw. entsprechenden Zwecken) ggf. in den USA verarbeitet (mit Blick auf die entsprechenden Verarbeitungen durch diese Kreditkartenunternehmen sind die jeweiligen Kreditkartenunternehmen die verantwortliche Stelle im datenschutzrechtlichen Sinn). Teilweise verwenden diese Kreditkartenunternehmen mit den Datenschutzbehörden abgestimmte sog. verbindliche interne Datenschutzvorschriften (Binding Corporate Rules), die sicherstellen, dass ein angemessenes Datenschutzniveau mit Blick auf Ihre in den USA verarbeiteten Daten besteht. Weitergehende Informationen zu diesen verbindlichen internen Datenschutzvorschriften erhalten Sie von den entsprechenden Kreditkartenunternehmen.

Soweit Kreditkartenunternehmen personenbezogene Daten des Nutzers in den USA verarbeiten, wird ein angemessenes Datenschutzniveau regelmäßig dadurch sichergestellt, dass entsprechende sog. EU-Standardvertragsklauseln beziehungsweise verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) verwendet werden, die sicherstellen, dass ein entsprechendes Schutzniveau erreicht wird. Weitere Informationen zu den entsprechenden Regelungen erhalten Sie von den entsprechenden Kreditkartenunternehmen.

Darüber hinaus ist eine Übermittlung der Zahlungsabwicklungsdaten an diese Unternehmen für die Abwicklung entsprechender Kreditkartenzahlungen erforderlich.

dd) Bevor Sie die App schließlich für Zahlungen bei Akzeptanzstellen einsetzen können, müssen Sie über die allgemeine Onlinebanking-Schnittstelle zu Ihrem Institut jeweils einmalig eine TAN (Transaktionsnummer) Ihres Instituts eingeben, damit das Institut verifizieren kann, dass es sich tatsächlich um den Nutzer handelt, der sich mit den Onlinebanking-Zugangsdaten in der App angemeldet hat. Diese TAN wird in der App nicht gespeichert.

ee) Zudem müssen Sie ggf. nach den Kartenbedingungen Ihres Instituts am POS-Terminal der Akzeptanzstelle Ihre kartenbezogene Geheimzahl Ihres Instituts (PIN) wie bei einem Einsatz der physischen Karte eingeben, um eine Zahlung ausführen zu können. Alternativ ist eine entsprechende Authentifizierung nach den Kartenbedingungen für individualisierte Authentifizierungsverfahren Ihres Instituts auch über die sog. Consumer Device Cardholder Verification Method (kurz: CDCVM) möglich. Als CDCVM bezeichnet man Methoden zur Authentifizierung des Nutzers über das mobile Endgerät des Nutzers unter Einsatz von Technologien zur Gesichtserkennung bzw. zur Erkennung Fingerabdrücken.

Bitte beachten Sie, dass weder S-Payment noch Ihr Institut in diesem Zusammenhang entsprechende Daten erhebt und / oder speichert (z.B. Fingerabdruck oder PIN). Die entsprechenden Prozesse laufen vollständig innerhalb der App ab. Die App wird jedoch eine Transaktion nur dann freigeben, wenn die entsprechende Transaktion über eine der vorgenannten Authentifizierungsmethoden bestätigt wurde. Weitergehende Informationen zu den vorgenannten Authentifizierungsmethoden finden Sie in der Dokumentation zu Ihrem Android-Betriebssystem bzw. zu Ihrem mobilen Endgerät.

ff) Wenn Sie die digitale Karte zur Bezahlung von Waren oder Dienstleistungen bei einer Akzeptanzstelle an der Kasse verwenden, übermittelt Ihr mobiles Endgerät einen die digitale Karte repräsentierenden, verschlüsselten Datensatz (der allerdings nicht den Namen des Nutzers enthält) an das POS-Terminal der Akzeptanzstelle.

Die Akzeptanzstelle übermittelt diese Daten sowie Zahlbetrag, Währung, Ort, Kassen- oder Terminal-ID, Zeitpunkt und Nummer des Vorgangs sowie Name und ggf. Filialbezeichnung der Akzeptanzstelle an Ihr Institut bzw. dessen technischen Dienstleister, damit die Zahlung abgewickelt werden kann.

gg) Ihnen können in der App ggf. bestimmte Informationen zu den von Ihnen durchgeführten Transaktionen zur Verfügung gestellt werden (insb. Bezahlbetrag und Bezahldatum), damit Sie einen Überblick über die bereits getätigten Transaktionen erhalten. Die entsprechenden Daten werden Ihnen von Ihrem Institut zur Verfügung gestellt. Bitte beachten Sie hierbei: Diese Transaktionshistorie stellt keinen rechtsgültigen Kontoauszug dar. Rechtsverbindliche Buchungen und Rechnungsabschlüsse erfolgen nur nach Maßgabe der Allgemeinen Geschäftsbedingungen Ihres Instituts.

c) Die App nutzt Teile der Google Firebase-Technologie von Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA („Google“). Die App verwendet die folgenden Google Firebase-Dienste:

- Firebase crashlytics („**FC**“): Wir sammeln unter Einsatz von FC im Falle eines technischen Fehlers oder Absturzes der App Daten zu diesem konkreten Ereignis (z.B. welche Funktion der App, welche Betriebssystemversion und welche Art von Gerät der Nutzer im Zeitpunkt des Auftreten des Fehlers genutzt hat). Die in diesem Zusammenhang erhobenen Daten

helfen uns, die App zu verbessern bzw. künftige Ausfälle und Störungen der App zu minimieren.

- Firebase Cloud Messaging („**FCM**"): FCM dient dazu, Push-Nachrichten (die nur innerhalb der App angezeigt werden) übermitteln zu können, damit wir dem Nutzer bestimmte (für ihn relevante Nachrichten) mitteilen können. Dabei wird dem mobilen Endgerät des Nutzers eine pseudonymisierte Push-Reference zugeteilt, die den Push-Nachrichten als Ziel dient.

- Firebase Remote Configuration („**FRC**"): Wir nutzen FRC. FRC ermöglicht die Konfiguration von App-Einstellungen, damit wir die App auf den Endgeräten, auf denen sie installiert ist, verändern können, ohne dass sie bei jeder Veränderung vollständig neu aus dem Google-Store installiert werden muss. In diesem Zusammenhang werden ggf. z.B. bestimmte Geräte-Informationen, verarbeitet. Informationen rund um die Funktionsweise von Remote Config finden Sie hier: *https://firebase.google.com/products/remote-config/*.

Weitere Informationen zu diesen Google Firebase-Diensten finden Sie auf den Webseiten von Google.

Die vorstehend genannten Daten werden ggf. auch auf bzw. über Server von Google (in den USA) verarbeitet. Wir haben mit Google eine Vereinbarung zur Auftragsverarbeitung betreffend die in diesem Zusammenhang ggf. verarbeiteten personenbezogenen Daten abgeschlossen (vgl. dazu auch unten unter Ziffer 4).

d) Rechtsgrundlage für die in Ziffer 3. a), b) aa), bb), cc) (betreffend die Abwicklung von Zahlungen), dd) und gg) genannte Verarbeitung und Übermittlung von personenbezogenen Daten durch S-Payment bzw. Ihr Institut ist Art. 6 Abs. 1 S. 1 lit. b) DSGVO (Vertragserfüllung und vorvertragliche Maßnahmen).

Rechtsgrundlage für die in Ziffer 3. b) cc) Abs. 1 genannten Verarbeitungen und Übermittlungen von personenbezogenen Daten betreffend Ihren Standort ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO (berechtigte Interessen; das berechtigte Interesse liegt darin, dass das entsprechende Kreditkartenunternehmen (z. B. Mastercard oder Visa) den Einsatz seiner digitalen Karten räumlich einschränken können muss (z. B. aufgrund regulatorischer Vorgaben in einzelnen Ländern oder Vorgaben der Kartensysteme). Zu diesem Zweck ist es notwendig, dass das entsprechende Kreditkartenunternehmen bereits in einem frühen Stadium erkennen kann, ob sich ein Nutzer der App in einem Land befindet, in dem digitale Karten nicht ausgewählt bzw. verwendet werden können) und (je nach Fall) Art. 46 Abs. 2 lit. b) bzw. Art. 47 DSGVO (bzw. ggf. Art. 49 Abs. 1 lit. b und c DSGVO).

Rechtsgrundlage für die in Ziffer 3. b) cc) Abs. 2 genannten Verarbeitungen und Übermittlungen von personenbezogenen Daten betreffend Root Detection ist (soweit es sich bei den in diesem Zusammenhang verarbeiteten Daten überhaupt um personenbezogene Daten handelt) Art. 6 Abs. 1 S. 1 lit. f) DSGVO (berechtigte Interessen; das berechtigte Interesse folgt aus dem in Ziffer 3. b) cc) Abs. 2 genannten Zweck – Missbrauchs- und Betrugsbekämpfung) und (je nach Fall) Art. 46 Abs. 2 lit. b) bzw. Art. 47 DSGVO (bzw. ggf. Art. 49 Abs. 1 lit. b) und c) DSGVO).

Rechtsgrundlage für die in Ziffer 3. c) genannten Verarbeitungen und Übermittlungen von personenbezogenen Daten (soweit es sich dabei überhaupt um personenbezogene Daten

handelt) ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO (berechtigte Interessen; die berechtigten Interessen ergeben sich aus den vorgenannten Zwecken).

4. Technische Dienstleistungen betreffend die App durch Subunternehmer

Für den Betrieb der App bzw. für die im Zusammenhang mit dem Einsatz der digitalen Karte abzuwickelnden Bezahlvorgänge werden von der S-Payment bzw. den Instituten ggf. externe Dienstleister eingesetzt, die personenbezogene Daten von Ihnen im Auftrag von S-Payment bzw. im Auftrag des Instituts verarbeiten. Diese Dienstleister verarbeiten die Daten ausschließlich nach den Weisungen von S-Payment bzw. von den Instituten (Auftragsverarbeiter). Rechtsgrundlage für die in dieser Ziffer 4 beschriebene Datenverarbeitung ist Art. 6 Abs. 1 S. 1 lit. b) DSGVO (Vertragserfüllung und vorvertragliche Maßnahmen) und Art. 28 DSGVO (Auftragsverarbeiter).

5. Dauer der Aufbewahrung Ihrer personenbezogenen Daten durch S-Payment

Soweit sich aus den übrigen Regelungen dieser Datenschutzerklärung keine andere Speicherdauer ergibt, speichert S-Payment Ihre von S-Payment im Zusammenhang mit der Nutzung der App bzw. das jeweilige Institut Ihre vom Institut mit dem Einsatz der digitalen Karte erlangten personenbezogenen Daten i.d.R. für die Dauer des jeweiligen Vertragsverhältnisses mit Ihnen (siehe für weitere Informationen zur Dauer der relevanten Vertragsverhältnisse (i) die Regelungen zur Vertragsdauer in den Lizenz- und Nutzungsbedingungen der App, und (ii) in den Kartenbedingungen und Allgemeinen Geschäftsbedingungen des jeweiligen Instituts), danach nur, in dem Umfang und soweit S-Payment bzw. das jeweilige Institut dazu aufgrund zwingender gesetzlicher Aufbewahrungspflichten verpflichtet ist. Soweit S-Payment bzw. das jeweilige Institut Ihre Daten nicht mehr für die oben beschriebenen Zwecke benötigt, werden sie während der jeweiligen gesetzlichen Aufbewahrungsfrist lediglich gespeichert und nicht für andere Zwecke verarbeitet.

6. Ihre Rechte

Sie haben das Recht, von S-Payment jederzeit Auskünfte über die zu Ihnen bei S-Payment gespeicherten personenbezogenen Daten zu verlangen. Sie haben das Recht von Ihrem kartenausgebenden Institut jederzeit Auskünfte über die zu Ihnen bei diesem Institut gespeicherten personenbezogenen Daten zu verlangen.

Soweit die gesetzlichen Voraussetzungen vorliegen, haben Sie gegenüber S-Payment bzw. gegenüber dem entsprechenden Institut ferner Rechte auf Berichtigung, Löschung bzw. Einschränkung der Verarbeitung der entsprechenden personenbezogenen Daten sowie das **Recht der Verarbeitung Ihrer personenbezogenen Daten durch S-Payment bzw. durch das entsprechende Institut zu widersprechen.** Wenn Sie eine Einwilligung zur Nutzung von personenbezogenen Daten erteilt haben, können Sie diese jederzeit (für die Zukunft) widerrufen.

Wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten durch S-Payment bzw. durch das entsprechende Institut gegen das anwendbare Datenschutzrecht verstößt, können Sie sich bei der zuständigen Aufsichtsbehörde für den Datenschutz beschweren.

7. Kontakt; Datenschutzbeauftragter; weitere Information

a) Sie können mit S-Payment unter der in Ziffer 1 angegeben Adresse sowie über datenschutz@s-payment.com Kontakt aufnehmen.

Für alle Fragen zum Thema Datenschutz bei S-Payment (einschl. der Geltendmachung Ihrer Rechte nach Ziffer 6) können Sie sich auch direkt an den Datenschutzbeauftragten von S-Payment wenden. Die Kontaktdaten des Datenschutzbeauftragten sind: S-Payment GmbH, Datenschutzbeauftragter, Am Wallgraben 115, 70565 Stuttgart, E-Mail: datenschutz@s-payment.com.

b) Weitere Informationen zu Ihrem kartenausgebenden Institut (insb. die Kontaktdaten), finden Sie in der App unter dem Punkt „Meine Sparkasse“. Dort finden Sie u. a. auch einen Link zu der Webseite des entsprechenden Instituts. Auf dieser Webseite finden Sie unter dem Punkt „Datenschutz“ die Kontaktdaten des Datenschutzbeauftragten des jeweiligen Instituts, an den Sie sich mit Ihren Fragen zum Thema Datenschutz wenden können (etwa zur Geltendmachung Ihrer Rechte nach Ziffer 6).

c) Weitergehende datenbezogene Informationen finden Sie auch unter www.sparkasse.de/kontaktloszahlen.

8. Datensicherheit

S-Payment und die Institute unterhalten aktuelle technische Maßnahmen zur Gewährleistung der Datensicherheit, insbesondere zum Schutz Ihrer personenbezogenen Daten vor Gefahren bei Datenübertragungen sowie vor Kenntniserlangung durch Dritte. Diese werden dem aktuellen Stand der Technik entsprechend jeweils angepasst.