EDEKABANK

**Anlage B) Datenverarbeitungsvereinbarung**

Für die Zwecke von Artikel 28(3) der Verordnung 2016/679 (der „DSGVO“)
Zwischen dem Händler und der EDEKABANK AG als Softwareanbieter werden die folgenden vertraglichen Klauseln (die „Klauseln“) vereinbart, um die Anforderungen der DSGVO zu erfüllen und den Schutz der Rechte der betroffenen Person zu gewährleisten.

## 1. Präambel

1.1. Diese Klauseln legen die Rechte und Pflichten des Datenverantwortlichen und des Datenverarbeiters bei der Verarbeitung personenbezogener Daten im Auftrag des Datenverantwortlichen fest.

1.2. Die Klauseln wurden entwickelt, um die Einhaltung von Artikel 28(3) der Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) durch die Parteien sicherzustellen.

1.3. Im Rahmen der Bereitstellung der SoftPOS Lösung wird der Datenverarbeiter personenbezogene Daten im Auftrag des Datenverantwortlichen gemäß den Klauseln verarbeiten.

1.4. Die Klauseln haben Vorrang vor ähnlichen Bestimmungen in anderen Vereinbarungen zwischen den Parteien.

1.5. Drei Anhänge sind den Klauseln beigefügt und bilden einen integralen Bestandteil der Klauseln.

1.6. Anhang A enthält Einzelheiten zur Verarbeitung personenbezogener Daten, einschließlich des Zwecks und der Art der Verarbeitung, der Art der personenbezogenen Daten, der Kategorien betroffener Personen und der Dauer der Verarbeitung.

1.7. Anhang B enthält die Bedingungen des Datenverantwortlichen für die Nutzung von Unterauftragsverarbeitern durch den Datenverarbeiter sowie eine Liste der vom Datenverantwortlichen genehmigten Unterauftragsverarbeiter.

1.8. Anhang C enthält die Anweisungen des Datenverantwortlichen zur Verarbeitung personenbezogener Daten, die vom Datenverarbeiter zu implementierenden Datenverarbeiter zu implementierenden Mindestsicherheitsmaßnahmen und die Durchführung von Audits des Datenverarbeiters und etwaiger Unterauftragsverarbeiter.

1.9. Die Klauseln sowie die Anhänge müssen von beiden Parteien schriftlich, auch in elektronischer Form, aufbewahrt werden.

1.10. Die Klauseln entbinden den Datenverarbeiter nicht von Verpflichtungen, denen der Datenverarbeiter gemäß der Datenschutz-Grundverordnung (DSGVO) oder anderer Gesetze unterliegt.

## 2. Die Rechte und Pflichten des Datenverantwortlichen

2.1. Der Datenverantwortliche ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit der DSGVO (siehe Artikel 24 DSGVO), den geltenden EU- oder nationalen Datenschutzbestimmungen[1] und den Klauseln erfolgt.

2.2. Der Datenverantwortliche hat das Recht und die Pflicht, Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu treffen.

2.3. Der Datenverantwortliche ist unter anderem dafür verantwortlich, dass die Verarbeitung personenbezogener Daten, die der Datenverarbeiter durchzuführen hat, eine Rechtsgrundlage hat.

[1] References to” Member States” made throughout the Clauses shall be understood as references to “EEA Member States”.

**3. Der Datenverarbeiter handelt nach Weisungen**

3.1. Der Datenverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisungen des Datenverantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaates, dem der Datenverarbeiter unterliegt, dazu verpflichtet. Solche Weisungen sind in den Anhängen A und C festgelegt. Weitere Weisungen können während der Dauer der Verarbeitung personenbezogener Daten durch den Datenverantwortlichen erteilt werden, müssen jedoch stets dokumentiert und schriftlich, auch in elektronischer Form, im Zusammenhang mit den Klauseln festgehalten werden.

3.2. Der Datenverarbeiter informiert den Datenverantwortlichen unverzüglich, wenn er der Auffassung ist, dass die Weisungen des Datenverantwortlichen gegen die DSGVO oder die geltenden EU- oder nationalen Datenschutzbestimmungen verstoßen.

**4. Vertraulichkeit**

4.1. Der Datenverarbeiter gewährt nur solchen Personen, die seiner Anweisung unterliegen, Zugriff auf die im Auftrag des Datenverantwortlichen verarbeiteten personenbezogenen Daten, die sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Vertraulichkeitspflicht unterliegen, und dies nur nach dem Prinzip der Notwendigkeit. Die Liste der Personen, denen Zugang gewährt wurde, wird regelmäßig überprüft. Nach dieser Überprüfung kann der Zugang zu personenbezogenen Daten entzogen werden, wenn der Zugang nicht mehr erforderlich ist, und personenbezogene Daten sind diesen Personen folglich nicht mehr zugänglich.

4.2. Der Datenverarbeiter muss dem Datenverantwortlichen auf dessen Anfrage nachweisen, dass die betreffenden Personen, die der Autorität des Datenverarbeiters unterliegen, der vorgenannten Vertraulichkeitspflicht unterliegen.

**5. Sicherheit der Verarbeitung**

5.1. Artikel 32 DSGVO sieht vor, dass unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Eintrittswahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen der Datenverantwortliche und der Datenverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen müssen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

Der Datenverantwortliche bewertet die Risiken für die Rechte und Freiheiten natürlicher Personen, die der Verarbeitung innewohnen, und ergreift Maßnahmen zur Minderung dieser Risiken:

a. Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste kontinuierlich sicherzustellen;
c. die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen;
d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

5.2. Gemäß Artikel 32 DSGVO bewertet der Datenverarbeiter auch – unabhängig vom Datenverantwortlichen – die Risiken für die Rechte und Freiheiten natürlicher Personen, die der Verarbeitung innewohnen, und ergreift Maßnahmen zur Minderung dieser Risiken. Zu diesem Zweck stellt der Datenverantwortliche dem Datenverarbeiter alle

Informationen zur Verfügung, die erforderlich sind, um solche Risiken zu identifizieren und zu bewerten.

5.3. Darüber hinaus unterstützt der Datenverarbeiter den Datenverantwortlichen bei der Einhaltung der Verpflichtungen des Datenverantwortlichen gemäß Artikel 32 DSGVO, indem er dem Datenverantwortlichen unter anderem Informationen über die bereits vom Datenverarbeiter gemäß Artikel 32 DSGVO umgesetzten technischen und organisatorischen Maßnahmen sowie alle weiteren Informationen zur Verfügung stellt, die der Datenverantwortliche zur Erfüllung seiner Verpflichtungen nach Artikel 32 DSGVO benötigt.

Wenn der Datenverantwortliche anschließend zu der Einschätzung gelangt, dass die Minderung der festgestellten Risiken weitere Maßnahmen erfordert, als der Datenverarbeiter bereits gemäß Artikel 32 DSGVO umgesetzt hat, legt der Datenverantwortliche diese zusätzlichen Maßnahmen, die in Anhang C zu implementieren sind, fest.

6. **Einsatz von Unterauftragsverarbeitern**

6.1. Der Datenverarbeiter muss die Anforderungen von Artikel 28(2) und (4) DSGVO erfüllen, um einen weiteren Verarbeiter (einen Unterauftragsverarbeiter) zu beauftragen.

6.2. Der Datenverarbeiter darf daher keinen weiteren Verarbeiter (Unterauftragsverarbeiter) ohne die vorherige allgemeine schriftliche Genehmigung des Datenverantwortlichen zur Erfüllung der Klauseln hinzuziehen.

6.3. Der Datenverarbeiter hat die allgemeine Genehmigung des Datenverantwortlichen zur Beauftragung von Unterauftragsverarbeitern. Der Datenverarbeiter informiert den Datenverantwortlichen schriftlich über jede beabsichtigte Änderung hinsichtlich der Hinzufügung oder des Austauschs von Unterauftragsverarbeitern mindestens 30 Tage im Voraus, um dem Datenverantwortlichen die Möglichkeit zu geben, solchen Änderungen vor der Beauftragung der betreffenden Unterauftragsverarbeiter zu widersprechen. Längere Vorankündigungsfristen für bestimmte Unterverarbeitungsdienste können in Anhang B vorgesehen werden. Die Liste der bereits vom Datenverantwortlichen genehmigten Unterauftragsverarbeiter befindet sich in Anhang B.

6.4. Beauftragt der Datenverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Namen des Datenverantwortlichen, so müssen dem Unterauftragsverarbeiter dieselben Datenschutzpflichten wie in den Klauseln auferlegt werden, insbesondere durch einen Vertrag oder eine andere Rechtsvorschrift gemäß EU-Recht oder dem Recht eines Mitgliedstaates, die ausreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen in einer Weise umgesetzt werden, dass die Verarbeitung den Anforderungen der Klauseln und der DSGVO entspricht.
Der Datenverarbeiter ist daher verantwortlich dafür, dass der Unterauftragsverarbeiter zumindest die Verpflichtungen erfüllt, denen der Datenverarbeiter gemäß den Klauseln und der DSGVO unterliegt.

6.5. Erfüllt der Unterauftragsverarbeiter seine Datenschutzverpflichtungen nicht, bleibt der Datenverarbeiter gegenüber dem Datenverantwortlichen voll verantwortlich für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters. Dies berührt nicht die Rechte der betroffenen Personen nach der DSGVO – insbesondere diejenigen, die in den Artikeln 79 und 82 DSGVO vorgesehen sind – gegenüber dem Datenverantwortlichen und dem Datenverarbeiter, einschließlich des Unterauftragsverarbeiters.

**7. Datenübermittlung in Drittländer oder an internationale Organisationen**

7.1. Jede Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen durch den Datenverarbeiter darf nur auf der Grundlage dokumentierter Anweisungen des Datenverantwortlichen erfolgen und muss stets im Einklang mit Kapitel V der DSGVO stehen.

7.2. Erfolgen Übermittlungen in Drittländer oder an internationale Organisationen, die der Datenverarbeiter nicht auf Anweisung des Datenverantwortlichen durchzuführen hat, aufgrund von EU- oder nationalem Recht, dem der Datenverarbeiter unterliegt, so informiert der Datenverarbeiter den Datenverantwortlichen über diese rechtliche Verpflichtung vor der Verarbeitung, es sei denn, dieses Recht verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.

7.3. Ohne dokumentierte Anweisungen des Datenverantwortlichen darf der Datenverarbeiter daher im Rahmen der Klauseln keine der folgenden Handlungen vornehmen:

a. personenbezogene Daten an einen Datenverantwortlichen oder einen Datenverarbeiter in einem Drittland oder einer internationalen Organisation übermitteln;
b. die Verarbeitung personenbezogener Daten an einen Unterauftragsverarbeiter in einem Drittland übertragen;
c. die personenbezogenen Daten durch den Datenverarbeiter in einem Drittland verarbeiten lassen.

7.4. Die Anweisungen des Datenverantwortlichen zur Übermittlung personenbezogener Daten in ein Drittland, einschließlich der gegebenenfalls nach Kapitel V DSGVO anwendbaren Übermittlungsinstrumente, sind in Anhang C.6. festzulegen.

7.5. Die Klauseln sind nicht mit den Standarddatenschutzklauseln im Sinne von Artikel 46(2)(c) und (d) DSGVO zu verwechseln, und die Klauseln können von den Parteien nicht als Übermittlungsinstrument gemäß Kapitel V DSGVO genutzt werden.

**8. Unterstützung des Datenverantwortlichen**

8.1. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Datenverarbeiter den Datenverantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Verpflichtungen des Datenverantwortlichen zur Beantwortung von Anfragen zur Ausübung der Rechte der betroffenen Person gemäß Kapitel III DSGVO. Dies bedeutet, dass der Datenverarbeiter den Datenverantwortlichen soweit möglich bei der Einhaltung folgender Rechte unterstützt:

a. Das Recht auf Information beim Erheben personenbezogener Daten von der betroffenen Person
b. Das Recht auf Information, wenn personenbezogene Daten nicht von der betroffenen Person erhoben, wurden
c. Das Recht der betroffenen Person auf Auskunft
d. Das Recht auf Berichtigung
e. Das Recht auf Löschung („Recht auf Vergessenwerden“)
f. Das Recht auf Einschränkung der Verarbeitung
g. Mitteilungs- und Benachrichtigungspflichten im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
h. Das Recht auf Datenübertragbarkeit
i. Das Widerspruchsrecht
j. Das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung, einschließlich Profiling, unterworfen zu werden.

8.2. Zusätzlich zur Unterstützung des Datenverantwortlichen gemäß Klausel 5.3. unterstützt der Datenverarbeiter den Datenverantwortlichen ferner – unter Berücksichtigung der Art

der Verarbeitung und der dem Datenverarbeiter zur Verfügung stehenden Informationen – bei der Einhaltung der folgenden Verpflichtungen:

a. Die Verpflichtung des Datenverantwortlichen, eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch 72 Stunden nach deren Kenntnis, der zuständigen Aufsichtsbehörde zu melden, es sei denn, die Verletzung ist voraussichtlich nicht mit Risiken für die Rechte und Freiheiten natürlicher Personen verbunden;
b. Die Verpflichtung des Datenverantwortlichen, die betroffene Person unverzüglich über die Verletzung des Schutzes personenbezogener Daten zu informieren, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt;
c. Die Verpflichtung des Datenverantwortlichen, eine Bewertung der Auswirkungen der vorgesehenen Verarbeitungsvorgänge auf den Schutz personenbezogener Daten durchzuführen (Datenschutz-Folgenabschätzung);
d. Die Verpflichtung des Datenverantwortlichen, die zuständige Aufsichtsbehörde zu konsultieren, bevor mit der Verarbeitung begonnen wird, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung ein hohes Risiko darstellt, es sei denn, der Datenverantwortliche ergreift Maßnahmen zur Minderung dieses Risikos.

8.3. Die Parteien legen in Anhang C die geeigneten technischen und organisatorischen Maßnahmen fest, durch die der Datenverarbeiter den Datenverantwortlichen unterstützt, sowie den Umfang und das Ausmaß der erforderlichen Unterstützung. Dies gilt für die Verpflichtungen in den Klauseln 8.1. und 8.2.

**9. Benachrichtigung bei Datenschutzverletzungen**

9.1. Im Falle einer Datenschutzverletzung muss der Datenverarbeiter den Datenverantwortlichen unverzüglich nach Bekanntwerden der Datenschutzverletzung benachrichtigen.

9.2. Die Benachrichtigung des Datenverarbeiters an den Datenverantwortlichen erfolgt, wenn möglich, innerhalb von 48 Stunden nach Bekanntwerden der Datenschutzverletzung, damit der Datenverantwortliche seiner Verpflichtung nachkommen kann, die Datenschutzverletzung gemäß Artikel 33 der DSGVO an die zuständige Aufsichtsbehörde zu melden.

9.3. In Übereinstimmung mit Klausel 8.2(a) unterstützt der Datenverarbeiter den Datenverantwortlichen bei der Meldung der Datenschutzverletzung an die zuständige Aufsichtsbehörde, indem der Datenverarbeiter dem Datenverantwortlichen die folgenden Informationen zur Verfügung stellt, die gemäß Artikel 33(3) DSGVO in der Meldung des Datenverantwortlichen an die Aufsichtsbehörde enthalten sein müssen:

a. Die Art der Datenschutzverletzung, einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl betroffener Personen sowie der Kategorien und der ungefähren Anzahl betroffener personenbezogener Datensätze;
b. Die wahrscheinlichen Folgen der Datenschutzverletzung;
c. Die Maßnahmen, die der Datenverantwortliche ergriffen, hat oder vorschlägt, um die Datenschutzverletzung zu beheben, einschließlich gegebenenfalls Maßnahmen zur Minderung der möglichen nachteiligen Auswirkungen.

9.4. Die Parteien legen in Anhang C alle Elemente fest, die der Datenverarbeiter zur Unterstützung des Datenverantwortlichen bei der Meldung einer Datenschutzverletzung an die zuständige Aufsichtsbehörde bereitstellen muss.

**10. Löschung und Rückgabe von Daten**

10.1. Nach Beendigung der Erbringung von Dienstleistungen zur Verarbeitung personenbezogener Daten ist der Datenverarbeiter verpflichtet, alle im Auftrag des Datenverantwortlichen verarbeiteten personenbezogenen Daten zu löschen und dem Datenverantwortlichen zu bestätigen, dass die Löschung erfolgt ist, es sei denn, das Unionsrecht oder das Recht eines Mitgliedstaates verlangt die Speicherung der personenbezogenen Daten.

**11. Audit und Inspektion**

11.1. Der Datenverarbeiter stellt dem Datenverantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Artikel 28 der DSGVO festgelegten Verpflichtungen und der Klauseln nachzuweisen, und ermöglicht sowie unterstützt Audits, einschließlich Inspektionen, die vom Datenverantwortlichen oder einem anderen vom Datenverantwortlichen beauftragten Prüfer durchgeführt werden.

11.2. Der Datenverarbeiter ist verpflichtet, den Aufsichtsbehörden, die gemäß den geltenden gesetzlichen Bestimmungen Zugang zu den Einrichtungen des Datenverantwortlichen und des Datenverarbeiters haben, oder deren Vertretern nach Vorlage einer entsprechenden Identifikation mit mindestens zwei Monaten Vorankündigung Zugang zu den physischen Einrichtungen des Datenverarbeiters zu gewähren.

11.3. Jede Anfrage bezüglich der DSGVO-Daten, DSGVO-Audit oder ähnlicher Anfragen wird dem Datenverantwortlichen nach Zeit- und Materialaufwand in Rechnung gestellt.

**12. Sonstige Vereinbarungen zwischen den Parteien**

12.1. Die Parteien können andere Klauseln zur Erbringung der Dienstleistungen zur Verarbeitung personenbezogener Daten vereinbaren, die beispielsweise die Haftung festlegen, solange diese Klauseln nicht direkt oder indirekt den Klauseln widersprechen oder die Grundrechte und Grundfreiheiten der betroffenen Personen sowie den durch die DSGVO gewährten Schutz beeinträchtigen.

**13. Beginn und Beendigung**

13.1. Die Klauseln treten am Tag der Unterzeichnung der Hauptvereinbarung in Kraft.

13.2. Beide Parteien haben das Recht, eine Neuverhandlung der Klauseln zu verlangen, wenn Änderungen der Rechtslage oder Unstimmigkeiten in den Klauseln Anlass zu einer solchen Neuverhandlung geben sollten.

13.3. Die Klauseln gelten für die Dauer der Erbringung der Dienstleistungen zur Verarbeitung personenbezogener Daten. Für die Dauer der Erbringung dieser Dienstleistungen können die Klauseln nicht gekündigt werden, es sei denn, die Parteien haben andere Klauseln zur Erbringung der Dienstleistungen zur Verarbeitung personenbezogener Daten vereinbart.

13.4. Wenn die Dienstleistungen zur Verarbeitung personenbezogener Daten beendet werden und die personenbezogenen Daten gemäß Klausel 10.1 und Anhang C.4 gelöscht oder an den Datenverantwortlichen zurückgegeben werden, können die Klauseln von jeder Partei durch schriftliche Mitteilung gekündigt werden.

## Anhang A – Informationen über die Verarbeitung

**A.1. Zweck der Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen:**

- Kreditkartentransaktionen und Quittungen, die in der mobilen Zahlungsanwendung des Datenverarbeiters generiert werden.
- Transaktionshistorie zu Supportzwecken.
- Ein Token, das aus der Kartennummer abgeleitet ist, und ein PAR-Wert, beide zur Unterstützung von Treuelösungen.

**A.2. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen betrifft hauptsächlich (Art der Verarbeitung):**

- Übermittlung von Daten an den Acquirer des Datenverantwortlichen und Versand von Quittungen per E-Mail.
- Transaktionshistorie für ein bestimmtes Terminal.
- Ein Token, das aus der Kartennummer abgeleitet ist, und ein PAR-Wert.

**A.3. Die Verarbeitung umfasst folgende Arten personenbezogener Daten über die betroffenen Personen:**

- E-Mail-Adresse
- Zahlungsdetails (Betrag, Geschäft, Zeitpunkt und Ergebnis)
- Kreditkarteninformationen (vollständiges Track-2-Äquivalent)
- PIN (verschlüsselt auf dem Client und im HSM umgewandelt)
- Ein Token, das aus der Kartennummer abgeleitet ist und für Treuelösungen verwendet werden kann, sowie ein PAR-Wert, der ebenfalls für Treuelösungen verwendet werden kann.

**A.4. Die Verarbeitung umfasst folgende Kategorien von betroffenen Personen:**

- Kreditkarteninhaber, die in einem der Geschäfte des Datenverantwortlichen unter Verwendung der mobilen Zahlungsanwendung des Datenverarbeiters einkaufen.

**A.5. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen kann ab Beginn der Klauseln durchgeführt werden. Die Verarbeitung hat folgende Dauer:**

1. Sehr sichere Daten (PIN-Block, sensible Track-2-Daten) werden nur so lange gespeichert, bis sie an den Acquirer/Verarbeiter übermittelt wurden.
2. Sichere Daten (PAN und Äquivalente) werden für die Dauer einer offenen Transaktion gespeichert. Eine abgeschlossene Transaktion bleibt offen, bis sie nicht mehr storniert werden kann. Dies wird durch die SVPA-Komponente gesteuert.
3. E-Mail-Adressen werden nicht gespeichert, sondern nur zum Versenden einer Quittung verwendet. Der E-Mail-Server speichert keine Kopien.
4. Teilweise anonymisierte Daten wie teilweise PAN- und Zahlungsdetails werden für 5 Jahre im Terminal-Transaktionsprotokoll gespeichert.
5. Ein Token, das aus der Kartennummer abgeleitet ist und für Treuelösungen verwendet werden kann, sowie ein PAR-Wert, der ebenfalls für Treuelösungen verwendet werden kann, werden maximal eine Stunde gespeichert.

## Anhang B – Autorisierte Unterauftragsverarbeite

### Appendix A
### B.1. Genehmigte Unterauftragsverarbeiter

Zu Beginn der Klauseln autorisiert der Datenverantwortliche die Beauftragung der folgenden Unterauftragsverarbeiter:

| NAME | FIRMENNUMMER | ADDRESS | BESCHREIBUNG DER VERARBEITUNG |
|---|---|---|---|
| Softpay ApS | CVR-Nr.: 41352272 | Lyngbyvej 28 3. Stock 2100 Kopenhagen Dänemark | Betrieb des Backendsystems zur Transaktionsverarbeitung über die SoftPOS Lösung. Alle Daten werden in Irland gespeichert und verarbeitet. |
| AWS EMEA SARL | B186284 | 38 Avenue John F. Kennedy, L-1855 Luxemburg | Speicherung und Verarbeitung von Daten. Alle Daten werden in Irland gespeichert und verarbeitet. |

Der Datenverantwortliche autorisiert zu Beginn der Klauseln die Nutzung der oben genannten Unterauftragsverarbeiter für die für diese Partei beschriebene Verarbeitung.

## Anhang C – Anweisungen zur Nutzung personenbezogener Daten

**Appendix B**

### C.1. Betreff/Anweisung für die Verarbeitung

Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen erfolgt durch den Datenverarbeiter, der die folgenden Aufgaben ausführt:

- Der Datenverarbeiter wird beauftragt, alle notwendigen Aufgaben zur Einleitung und zum Abschluss der Transaktion in der mobilen Zahlungsanwendung von Softpay auszuführen, einschließlich des Versands von Quittungen.
- Der Transaktionsablauf ist im Systemdiagramm dargestellt.
- Es liegt in der Verantwortung des Distributors und seiner Partner sowie Kunden, eine
- Datenverarbeitungsvereinbarung mit ihren POS- oder ECR-Anbietern abzuschließen, die sich auf die von der SoftPOS Produktlösung an solche Systeme übertragenen Daten beziehen.

### C.2. Sicherheit der Verarbeitung

Das Sicherheitsniveau muss Folgendes berücksichtigen:

- Alle personenbezogenen Daten außer E-Mail-Adressen fallen in den Geltungsbereich und werden durch den PCI-DSS-Standard geregelt.
- E-Mails werden während der Übertragung verschlüsselt und nach dem Versand der Quittung nicht gespeichert.
- Der aus der Kartennummer abgeleitete Token und der PAR-Wert, die beide für Treuelösungen verwendet werden, werden nur im Speicher gespeichert und sind kurzlebig.

### C.3. Unterstützung des Datenverantwortlichen

Der Datenverarbeiter unterstützt den Datenverantwortlichen soweit möglich – im Umfang und Ausmaß der unten festgelegten Unterstützung – gemäß Klausel 8.1. und 8.2. durch die Umsetzung der folgenden technischen und organisatorischen Maßnahmen:

- Der Datenverarbeiter hat einen Datenschutzbeauftragten (DPO) benannt, der als Anlaufstelle für alle Anfragen oder Informationen zu personenbezogenen Daten fungiert. Es liegt in der Verantwortung des DPO, den Datenverantwortlichen gemäß den Klauseln 8.1 und 8.2 zu informieren und zu unterstützen.

### C.4. Aufbewahrungsfristen/Löschverfahren

1. Sehr sichere Daten (PIN-Block, sensible Track-2-Daten) werden nur so lange gespeichert, bis sie an den Acquirer übermittelt wurden.
2. Sichere Daten (PAN und Äquivalente) werden für die Dauer einer offenen Transaktion gespeichert. Eine abgeschlossene Transaktion bleibt offen, bis sie nicht mehr storniert werden kann. Dies wird durch die SVPA-Komponente gesteuert.
3. E-Mail-Adressen werden nicht gespeichert, sondern nur zum Versenden einer Quittung verwendet. Der E-Mail-Server speichert keine Kopien.
4. Teilweise anonymisierte Daten wie teilweise PAN- und Zahlungsdetails werden für 5 Jahre im Terminal-Transaktionsprotokoll gespeichert.
5. Ein Token, das aus der Kartennummer abgeleitet ist und für Treuelösungen verwendet werden kann, sowie ein PAR-Wert, der ebenfalls für Treuelösungen verwendet werden kann, werden maximal eine Stunde gespeichert.

### C.5. Verarbeitungsstandort

Die Verarbeitung der personenbezogenen Daten im Rahmen der Klauseln darf nur an den folgenden Standorten erfolgen, es sei denn, der Datenverantwortliche hat dies zuvor schriftlich genehmigt:

- Amazon AWS Irland

- Datenverarbeiter dänisches Büro

**C.6. Anweisungen zur Übermittlung personenbezogener Daten in Drittländer**
Sofern der Datenverantwortliche in den Klauseln oder danach keine dokumentierten Anweisungen zur Übermittlung personenbezogener Daten in ein Drittland erteilt, ist der Datenverarbeiter nicht berechtigt, eine solche Übermittlung im Rahmen der Klauseln durchzuführen.

**C.7. Verfahren für Audits, einschließlich Inspektionen der Verarbeitung personenbezogener Daten durch den Datenverarbeiter**
Der Datenverantwortliche oder seine Vertreter können eine physische Inspektion der Orte durchführen, an denen die Verarbeitung personenbezogener Daten durch den Datenverarbeiter stattfindet, um die Einhaltung der DSGVO, der geltenden EU- oder nationalen Datenschutzbestimmungen und der Klauseln durch den Datenverarbeiter zu überprüfen.

Die Kosten des Datenverantwortlichen für die Inspektion trägt der Datenverantwortliche.

**C.8. Verfahren für Audits, einschließlich Inspektionen der Verarbeitung personenbezogener Daten durch Unterauftragsverarbeiter**
Der Datenverarbeiter oder seine Vertreter können eine physische Inspektion der Orte durchführen, an denen die Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter stattfindet, um die Einhaltung der DSGVO, der geltenden EU- oder nationalen Datenschutzbestimmungen und der Klauseln durch den Unterauftragsverarbeiter zu überprüfen.

Für Amazon AWS verlässt sich der Datenverarbeiter auf die von Amazon AWS bereitgestellten Berichte.
Die Kosten des Datenverantwortlichen für die Inspektion trägt der Datenverantwortliche.