VERTRAG ZUR AUFTRAGSVERARBEITUNG

betreffend die Vereinbarung

NUTZUNG DER E-COMMERCE PLATTFORM SUPR

(„Hauptvertrag“)

zwischen

SUPR-Händler
(„Auftraggeber“)

und der

Wirecard Technologies GmbH
Einsteinring 35
85609 Aschheim
(„Auftragnehmer“ oder “Wirecard“).

1. GEGENSTAND UND DAUER DER AUFTRAGSVERARBEITUNG

1) Die vorliegende Vereinbarung zur Auftragsverarbeitung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für den Auftragnehmer und den Auftraggeber aus dem anwendbaren Datenschutzrecht und insbesondere aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) sowie aus den anwendbaren nationalen Umsetzungsgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber im Rahmen des Hauptvertrages personenbezogene Daten verarbeitet.
2) Gegenstand und Zweck der Auftragsverarbeitung für den Auftraggeber ist das Betreiben eines Webshops („SUPR Onlineshop“) über die E-Commerce Plattform SUPR („SUPR“).
Mit SUPR können Verkäufer, Dienstleistungsanbieter oder sonstige Unternehmer einen eigenen Onlineshop erstellen, anpassen und verwalten. Zudem bietet SUPR die technische Möglichkeit, Leistungen von ausgewählten Dritten mit dem jeweiligen SUPR Onlineshop technisch zu verknüpfen und so zu nutzen.
3) Die Dauer der Auftragsverarbeitung umfasst die Laufzeit des Hauptvertrags, in dessen Rahmen diese Vereinbarung zur Auftragsdatenvereinbarung („Vereinbarung“) getroffen wurde.

2. AUFTRAGSINHALT

1) Art und Zweck der vorgesehenen Erhebung, Verarbeitung und Nutzung von Daten sind

- die Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag zur Nutzung von SUPR

2) Art der Daten sind

- Informationen über den Endkunden des Auftraggebers (z.B. Vor- und Nachname, Rechnungs- und Lieferadresse, E-Mail-Adresse, IP Adresse)

Folgende Daten der Endkunden des Auftraggebers werden im Einzelnen erhoben und verarbeitet:

- E-Mail-Adresse
- Anrede
- Vorname / Nachname
- Rechnungs- und Lieferadresse
- IP Adresse

- Informationen zu der gewählten Zahlungsart des Endkunden (z.B. Kreditkarte)
- Informationen zur Transaktion (z.B. Ware, Artikelnummer, Kaufpreis und ähnliche Informationen, die im Admin-Bereich des Webshops verwaltet werden)
- Informationen über aktuelle und vergangene Transaktionen des Endkunden

soweit sie zur Erfüllung der o.a. Zwecke benötigt werden.

3) Betroffene sind Endkunden des Auftraggebers.

3. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1) Für die ordnungsgemäße Umsetzung der in vorbezeichneter Vereinbarung zwischen den Parteien geregelten Auftragsverarbeitung durch den Auftragnehmer hat dieser geeignete technische und organisatorische Maßnahmen zur Datensicherung im Sinne von Art 28, 32 DS-GVO getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Eine Übersicht der zum Zeitpunkt der Auftragsvergabe getroffenen Maßnahmen wird dem Auftraggeber mit dieser Vereinbarung als **Anlage 1** zur Verfügung gestellt.
2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, getroffene Maßnahmen weiterzuentwickeln und/oder mit adäquaten Alternativen zu ersetzen. Dabei darf das gesetzlich vorgeschriebene Datenschutzniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer stellt dem Auftraggeber jederzeit auf Anfrage Informationen zu den angewandten technischen und organisatorischen Maßnahmen zur Verfügung.

4. RECHTE DER BETROFFENEN

Der Auftragnehmer wird den Auftraggeber nach Weisung des Auftraggebers bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte eines Betroffenen nach Kapitel III der DS-GVO nach Möglichkeit unterstützen und die hierfür geeigneten und erforderlichen technischen und organisatorischen Maßnahmen treffen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Wahrnehmung seiner Rechte bezüglich seiner personenbezogenen Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt, erstattet der Auftraggeber dem Auftragnehmer Kosten und Aufwand.

5. PFLICHTEN DES AUFTRAGNEHMERS

1) Der Auftragnehmer wird die personenbezogenen Daten nur auf Weisung, also die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit Daten gerichtete dokumentierte Anordnung des Auftraggebers, verarbeiten (einschließlich der Übermittlung), es sei denn, er ist zur Verarbeitung gesetzlich verpflichtet; in diesem Fall wird er dem Auftraggeber diese gesetzliche Anforderung vorab mitteilen, es sei denn, eine solche Mitteilung ist aufgrund eines wichtigen öffentlichen Interesses untersagt.
2) Der Auftragnehmer gewährleistet, dass die bei der Datenverarbeitung eingesetzten Mitarbeiter des Auftragnehmers schriftlich zur Vertraulichkeit gemäß Art. 28 Abs. 3 b) DS-GVO verpflichtet worden sind oder einer angemessenen gesetzlichen Schweigepflicht unterliegen. Soweit der Auftraggeber weiteren Geheimhaltungspflichten, etwa nach berufsrechtlichen, strafrechtlichen oder prozessrechtlichen Vorschriften, unterliegt, klärt er den Auftragnehmer hierüber auf und unterweist ihn und seine Mitarbeiter auf Verlangen in der Anwendung der Geheimhaltungspflichten.
3) Die technischen und organisatorischen Maßnahmen, wie unter Ziffer 3 dieser Vereinbarung und in der Anlage 1 hierzu definiert, werden vom Auftragnehmer umgesetzt und eingehalten. Hierzu gehören insbesondere

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und

Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4) Soweit keine Verfahrenserwägungen entgegenstehen, wird der Auftragnehmer den Auftraggeber über aufsichtsrechtliche Maßnahmen der zuständigen Aufsichtsbehörde nach Art. 58 DS-GVO sowie über gerichtliche Entscheidungen im Zusammenhang mit den Art. 83, 84 DS-GVO informieren.
5) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt und wird diesen gegenüber dem Auftraggeber schriftlich oder per Email benennen.
6) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit die von ihm übermittelten personenbezogenen Daten und Unterlagen betroffen sind. Nicht mehr erforderliche Daten sind beim Auftragnehmer unter Maßgabe von Ziffer 4 dieser ergänzenden Bestimmungen unverzüglich zu löschen. Eventuelle über diese ergänzenden Bestimmungen hinausgehende Kontrollen richten sich allein nach den gesetzlichen Vorschriften.

6. UNTERSTÜTZUNG NACH ART. 32 BIS 36 DS-GVO

Der Auftragnehmer wird den Auftraggeber auf Anfrage im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach den Art. 32 bis 36 DS-GVO mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Dies betrifft u.a. die Wahrnehmung der Betroffenenrechte, die Sicherheit der Verarbeitung, die Meldung von Datenschutzverstößen und entsprechende Benachrichtigung der Betroffenen, die Unterstützung bei Kontrollen durch die zuständigen Aufsichtsbehörden, sowie bei der Datenschutz-Folgeabschätzung. Der Auftraggeber wird den Auftragnehmer für dessen Unterstützung von allen hiermit zusammenhängenden Unkosten und Aufwand freistellen, es sei denn, die kosten/aufwandverursachenden Maßnahmen wurden vom Auftragnehmer verschuldet. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, in vollem Umfang, und der Aufwand erstattet.

7. BEGRÜNDUNG VON UNTERAUFTRAGSVERHÄLTNISSEN

1) Der Auftragnehmer darf zur Erfüllung der vertraglichen Leistungen Teile der Verarbeitung an Unterauftragnehmer vergeben. Folgende Unterauftragnehmer sind zum Zeitpunkt des Vertragsschlusses mit der Erbringung von vertragsrelevanten Leistungen beauftragt:

Firma Unterauftrag-nehmer	**Anschrift/Land**	**Leistung**
CleverReach® USA (Campaign Monitor)	154 Grand St New York, NY 10013 USA	Newslettersystem / Mailversand aller systemseitigen E-Mails
Slack	500 Howard Street, San Francisco, CA 94105, United States of America	Mitarbeiter-Chat, es können dort Daten der B2B-Kunden gespeichert werden (keine Endkundendaten)
Freshworks Inc.	1250 Bayhill Drive Suite 315 San Bruno, CA 94066 USA	Helpdesk-SaaS / CRM-System
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 United States	Hosting Wirecard Infrastruktur / Failover-System. Ausschließlich auf Servern in der Region Europa/Frankfurt

Der Auftraggeber erklärt sich mit der Unterbeauftragung der vorgenannten Unternehmen einverstanden. Ebenso ist der Auftraggeber mit der Unterbeauftragung weiterer Unternehmen einverstanden, sofern die Verpflichtungen dieser Vereinbarung an die Unterauftragnehmer weitergegeben werden und dabei mindestens dasselbe Schutzniveau eingehalten wird.

2) Bei der Einbindung von weiteren Unterauftragnehmern wird der Auftragnehmer den Auftraggeber informieren. Der Auftraggeber darf hinzukommende Unterauftragnehmer des Auftragnehmers nur dann ablehnen, soweit hierfür ein zwingender datenschutzrechtlicher Grund vorliegt und dies unverzüglich nach der Information schriftlich an den Auftragnehmer kommuniziert wurde. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer als Nebenleistung zur Unterstützung bei der Auftragsdurchführung von Dritten in Anspruch nimmt. Hierzu zählen Telekommunikationsdienstleistungen einschließlich Housing sowie Übermittlung und Hosting von Daten, Transport- und Kommunikationsdienstleistungen, Reinigungskräfte sowie Datenträger- und Dokumententsorgung.
3) Der Auftragnehmer schließt im Rahmen der Unterauftragsverhältnisse die datenschutzrechtlich erforderlichen Verträge. Dem Auftragnehmer ist es gestattet, die Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten oder durch Unterauftragnehmer verarbeiten zu lassen, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und ihm die Einhaltung der technischen und organisatorischen Maßnahmen auf Verlangen nachweist. Auf etwaige Unterauftragnehmer ist diese Ziffer 7 vollumfänglich anwendbar. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit Unterauftragnehmern Verträge – etwa (Unter-) Auftragsverarbeitungsverträge und EU-Standardvertragsklauseln oder ähnliche Verträge – abzuschließen, die erforderlich sind, um hinsichtlich des Datentransfers ein angemessenes Datenschutzniveau zu gewährleisten. Der Auftragnehmer darf Unterauftragnehmern Untervollmachten erteilen. Der Auftraggeber wird den Auftragnehmer unentgeltlich und im erforderlichen und zumutbaren Maß an der Erfüllung der rechtlichen Voraussetzungen für den Datentransfer unterstützen.

8. KONTROLLRECHTE DES AUFTRAGGEBERS

1) Der Auftraggeber hat sich von der ordnungsgemäßen Verarbeitung seiner personenbezogenen Daten sowie von der Einhaltung der beim Auftragnehmer vor Ort getroffenen technischen und organisatorischen Datensicherungsmaßnahmen zu überzeugen. Hierzu wird der Auftragnehmer auf Anfrage des Auftraggebers die Einhaltung der technischen und organisatorischen Maßnahmen durch geeignete Dokumentation wie z.B. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, externe Datenschutzauditoren) oder eine Zertifizierung durch IT- Sicherheits- oder Datenschutzaudit und/ oder anerkannten Zertifizierungen nach ISO 27001 nachweisen.
2) Der Auftragnehmer wird dem Auftraggeber oder einem von diesem beauftragten unabhängigen externen Prüfer die Überprüfung, einschließlich Inspektion, ermöglichen und hierzu beitragen, insbesondere wenn es z.B. einen Sicherheitsvorfall gab und /oder eine Überprüfung, einschließlich Inspektion, vom Gesetzgeber oder von einer Datenschutzbehörde verlangt wird. Zu einer solchen Überprüfung, einschließlich Inspektion, darf der Auftraggeber oder sein beauftragter unabhängiger Dritter nach Anmeldung im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter Beachtung der Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers und eventueller Unterauftragnehmer die Geschäftsräume des Auftragnehmers, in denen Daten des Auftraggebers verarbeitet werden, betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen nach Anlage 1 zu überzeugen.
3) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.
4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Auf Verlangen hat der Auftraggeber

dem Auftragnehmer die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.
5) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder vertragliche Regelungen verstoßen würde. Insbesondere erhält der Auftraggeber keinen Zugang zu Informationen über andere Geschäftspartner des Auftragnehmers, über Kosten, über Qualitätsprüfungs- und Vertragsmanagementberichte sowie über sämtliche andere nichtöffentliche Informationen des Auftragnehmers, die für gesetzliche Kontrollrechte nicht unmittelbar erforderlich sind.
6) Der Auftraggeber erstattet dem Auftragnehmer dessen Kosten und Aufwendungen des Nachweises der Einhaltung der technischen und organisatorischen Maßnahmen, insbesondere den Aufwand für etwaige Vor-Ort-Überprüfungen und Inspektionen.

9. MITTEILUNG BEI VERSTÖSSEN DES AUFTRAGNEHMERS

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt wird. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene und spricht sich hierfür unverzüglich mit dem Auftraggeber ab.

10. VERANTWORTLICHKEIT UND WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

1) Der Auftraggeber ist verantwortliche Stelle für die Verarbeitung der Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber. Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung in der erforderlichen Qualität zur Verfügung zu stellen.
2) Der Auftragnehmer verpflichtet sich, die Verarbeitung der ihm übergebenen personenbezogenen Daten im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers durchzuführen.
3) Der Auftragnehmer und seine Unterauftragnehmer dürfen die Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke verarbeiten, soweit das Gesetz oder eine Einwilligung des Betroffenen dies gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung. In jedem Fall dürfen der Auftragnehmer und seine Unterauftragnehmer die Daten in anonymisierter Form für eigene Zwecke verarbeiten.
4) Der Auftraggeber trägt aufgrund von Weisungen anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.
5) Aus Gründen der Nachvollziehbarkeit haben sämtliche Weisungen des Auftraggebers schriftlich oder in Textform (z. B. per E-Mail) zu erfolgen bzw. muss jede mündliche Weisung unverzüglich schriftlich oder in Textform bestätigt werden.
6) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen die DS-GVO, das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, darf er die Ausführung der Weisung verweigern, bis der Auftraggeber die Weisung bestätigt oder in eine datenschutzkonforme Weisung geändert hat.

11. LÖSCHUNG VON DATEN UND RÜCKGABE VON DATENTRÄGERN

Nach Beendigung des Auftragsverhältnisses ist der Auftragnehmer verpflichtet, die ihm in Zusammenhang mit dem Hauptvertrag übergebenen und noch nicht gelöschten personenbezogenen Daten nach Wahl des Auftraggebers zu löschen, zu sperren oder an den Auftraggeber zurückzugeben. Gesetzliche, behördliche, satzungsgemäße, vertragliche und andere Aufbewahrungspflichten bleiben unberührt.

12. ANSPRECHPARTNER IN SACHEN DATENVERARBEITUNG BZW. DATENSCHUTZ

Seitens des Auftraggebers:
der SUPR-Händler selbst, sofern nichts Gegenteiliges bekannt gegeben wurde.

Seitens des Auftragnehmers:
Externer betrieblicher Datenschutzbeauftragter: Dr. Felix Wittern, Fieldfisher (Germany) LLP, Am Sandtorkai 68, 20457 Hamburg

ANLAGE 1

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN DER WIRECARD-GRUPPE

Die Wirecard-Gruppe („Wirecard“) hat unter Berücksichtigung des Standes der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete Maßnahmen ergriffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zu diesem Zweck hat Wirecard die Schutzziele des Art. 32 (1) DSGVO wie die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Diensten sowie deren Belastbarkeit im Zusammenhang mit der Art, dem Umfang, den Umständen und dem Zweck der Verarbeitung beachtet. Wirecard hat auch ein Verfahren für die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen implementiert, um die Sicherheit der Verarbeitung sicherzustellen.
Im Folgenden werden die Maßnahmen erläutert, die zur Gewährleistung der Einhaltung der einzelnen Kontrollen ergriffen wurden.

Pseudonymisierung (Art. 32 (1) a) DSGVO)	**Wirecard pseudonymisiert in der Regel in Form von Verschlüsselung, wo dies notwendig und relevant ist.**
Verschlüsselung (Art. 32 (1) a) DSGVO)	Der Austausch und die Übermittlung personenbezogener Daten erfolgt grundsätzlich nur in verschlüsselter Form. Beim Austausch personenbezogener Daten ist die Verschlüsselung zentrales Thema der allgemeinen Datenschutzschulungen, die für jeden Mitarbeiter verpflichtend sind. Sämtliche Schnittstellen zu externen Stellen, die personenbezogene Daten in automatisierter Form übermitteln, sind nach neuesten Standards gesichert, z. B. durch TLS-Verschlüsselung. • Mobile Computer (Laptops) sind mit Festplattenverschlüsselung ausgestattet. • Je nach Art der Datenübertragung werden verschlüsselte Übertragungsprotokolle über HTTPS, TLS v1.1 oder v1.2 und SFTP, SSH v2 verwendet. • E-Mails und Dateien können verschlüsselt sein (z. B. PGP-Verschlüsselung für den regelmäßigen, verschlüsselten Datenaustausch). • Daten von Kreditkarten werden in den Systemen von Wirecard in verschlüsselter Form gespeichert. • Wirecard verwendet starke Verschlüsselungsalgorithmen, die in den internationalen Sicherheitsstandards wie NIST und PCI DSS festgelegt sind. • Verschlüsselungsschlüssel sind vor dem allgemeinen Zugriff geschützt. Nur zugelassene Custodians können auf die Verschlüsselungskomponenten zugreifen.

	• Verschlüsselungsschlüssel, die mit bewährten starken kryptographischen Algorithmen zur Erzeugung von Zufalls- oder Pseudozufallszahlen generiert wurden, werden jederzeit in einer der folgenden Formen gespeichert:
	
	  • Verschlüsselt mit einem Key Encrypting Key (KEK), der mindestens so stark wie der Datenverschlüsselungsschlüssel ist;
	
	  • Mindestens zwei Schlüsselkomponenten in voller Länge (kein Schlüssel-Custodian kennt oder hat Zugriff auf alle Datenverschlüsselungsschlüssel);
	
	  • Innerhalb eines kryptographischen Hardware-Sicherheitsmoduls (HSM).
	
	• Sämtliche Datenverschlüsselungsschlüssel werden nach Ablauf der Kryptoperiode geändert oder wenn besondere Umstände wie der Austritt des Schlüssel-Custodians eine Änderung zur Aufrechterhaltung der Schlüsselintegrität vorschreiben.
	
	• Entwicklung/Testsysteme sind von den Produktionsumgebungen mit einer Zugriffskontrolle getrennt, um die Trennung durchzusetzen.
	
	• Produktionsdaten (Live-PAN) werden nicht zu Testzwecken verwendet.

Vertraulichkeit (Art. 32 (1) b) DSGVO)	**ZUGANG ZU RÄUMLICHKEITEN** • Alle Räumlichkeiten von Wirecard verfügen über ein Zutrittssystem mit Chipkarten. Es wird zwischen den Eingängen zu verschiedenen Bereichen innerhalb der Gebäude unterschieden. Alle Mitarbeiter erhalten Chipkarten mit den für ihre Arbeit erforderlichen Zutrittsrechten. Die von der Abteilung Facility Management gewährten Zutrittsrechte werden dokumentiert und von der IT-Sicherheit in regelmäßigen Abständen überprüft. Besucher dürfen sich durch die Büroräumlichkeiten nur in Begleitung bewegen und erhalten separate Ausweise. • Alle Eingänge zu den Gebäuden von Wirecard werden mit Videokameras überwacht. • Der Zutritt zu Rechenzentren unterliegt strengen Vorschriften. Jeder Zutritt zu den Rechenzentren erfordert eine separate Anmeldung. Dies gilt auch für Mitarbeiter von Wirecard. Die Anmeldungen erfolgen durch die Leiter der IT-Abteilung und sind fälschungssicher (authentifiziert). • Dritte dürfen die Rechenzentren nur in Ausnahmefällen betreten und müssen von Mitarbeitern von Wirecard begleitet werden. Jeder Zutritt wird revisionssicher protokolliert. Die Zugriffsprotokolle werden von der IT-Sicherheit in regelmäßigen Abständen überprüft. • Die Rechenzentren werden vor unbefugtem Zutritt durch Sicherheitspersonal, das rund um die Uhr vor Ort ist, sowie durch Videokameras und Alarmsysteme geschützt. **KONTROLLE DES SYSTEMZUGRIFFS** • Alle Systeme bei Wirecard sind mit Zugriffskontrollsystemen ausgestattet.

	• Der Systemzugriff ist für jeden Mitarbeiter von Wirecard personalisiert. Der Zugriff ist durch persönliche Passwörter geschützt, die nur der jeweilige Mitarbeiter kennt. Die Passwortrichtlinie erfordert die Änderung von persönlichen Passwörtern in regelmäßigen Abständen (je nach System wurden Zeiträume von 90 Tagen oder weniger festgelegt) und stellt die Qualität und Komplexität des Passwortes durch speziell definierte Regeln sicher. Alle Regeln zur Vergabe und Änderung von Passwörtern wurden schriftlich festgelegt und entsprechen den verbindlichen PCI-DSS-Vorschriften. • Die Bildschirme an allen Arbeitsplätzen und alle Dienste, die für die Verarbeitung und Speicherung von personenbezogenen Daten genutzt werden, werden nach 15 Minuten Inaktivität automatisch gesperrt. Eine Entsperrung ist nur mit dem persönlichen Passwort durch wiederholtes Einloggen möglich. Darüber hinaus wird jede Sperrung des Arbeitsplatzrechners bei Verlassen des Arbeitsplatzes durch eine interne Richtlinie verbindlich geregelt. **KONTROLLE DES DATENZUGRIFFS** • Die Zugriffskontrolle basiert auf einem System von Rollen und Rechten, das zur Gewährleistung des Need-to-know-Prinzips bei jedem Datenzugriff angewendet wird. So hat jeder Mitarbeiter Zugriff auf genau die Daten, die er bzw. sie für seine bzw. ihre tägliche Arbeit benötigt. • Rechte, die für die jeweilige Stelle des Mitarbeiters erforderlich sind, sind in Form von an den Mitarbeiter zugewiesenen Rollen definiert. Weitere Einzelberechtigungen müssen von der IT-Sicherheit freigegeben werden. Die Autorisierung erfolgt nach Rücksprache mit dem Informationseigner (in der Regel der Leiter der zuständigen Fachabteilung) und im Rahmen der datenschutzrechtlichen Vorgaben. • Die Zuweisung von Rechten wird nachvollziehbar dokumentiert. • Die Rollenbeschreibungen und zugewiesenen Rechte werden von den zuständigen Abteilungen dokumentiert und gepflegt sowie in regelmäßigen Abständen (mindestens einmal jährlich) von der IT-Sicherheit stichprobenartig überprüft. • Administratorzugriffsrechte werden erst nach einer vorherigen internen Schulung erteilt. Jeder Administratorzugriff wird gemäß den PCI-DSS-Vorschriften revisionssicher protokolliert. • Durch die regelmäßige und zeitnahe Installation von Sicherheitsupdates für alle verwendeten Drittanwendungen wird sichergestellt, dass Unbefugte keinen Zugriff auf die Daten erhalten; die IT-Betriebssysteme (OS) werden gemäß den PCI-DSS-Vorschriften mit monatlichen Sicherheitsupdates versorgt.
Integrität (Art. 32 (1) b) DSGVO)	Der Austausch und die Übermittlung personenbezogener Daten erfolgt grundsätzlich nur in verschlüsselter Form. Je nach Art der Datenübertragung werden verschlüsselte Übertragungsprotokolle über HTTPS, TLS v1.1 oder v1.2 und SFTP, SSH v2 verwendet. E-Mails und Dateien können verschlüsselt sein (z. B. PGP-Verschlüsselung für den regelmäßigen, verschlüsselten Datenaustausch). Darüber hinaus wurde ein System implementiert, das die sichere einmalige Übermittlung von personenbezogenen Daten gewährleistet (Datenraumprinzip).

	• Beim Austausch personenbezogener Daten ist die Verschlüsselung zentrales Thema der allgemeinen Datenschutzschulungen, die für jeden Mitarbeiter verpflichtend sind. Sämtliche Schnittstellen zu externen Stellen, die personenbezogene Daten in automatisierter Form übermitteln, sind nach neuesten Standards gesichert, z. B. durch TLS-Verschlüsselung. • Alle Schnittstellen sind dokumentiert. Die externen Dokumentationen der Schnittstellen sind verfügbar. • Medienbestände und eine Clean-Desk-Policy verhindern eine unbefugte Einsichtnahme sowie den Diebstahl von Speichermedien und Dokumenten. In der Regel werden Speichermedien und Dokumente, die besondere personenbezogene Daten enthalten, per Kurierdienst gesendet, wobei die Speichermedien verschlüsselt sind. • Im Falle eines Administratorzugriffs werden sämtliche Änderungen, die an den personenbezogenen Daten in den Systemen von Wirecard vorgenommen werden, von der jeweiligen Softwareanwendung erfasst oder auf Basis entsprechender Verfahren dokumentiert, um zu gewährleisten, dass sämtliche Änderungen jederzeit nachvollziehbar sind. • Für die Dateneingabe und -änderung erhält jeder Mitarbeiter einen persönlichen Benutzernamen für das jeweilige System, um sicherzustellen, dass alle Eingaben einer bestimmten Person zugeordnet werden können. • Die Qualität der von Wirecard entwickelten Anwendungen wird vor der Implementierung durch ein umfassendes Qualitätssicherungsverfahren sichergestellt.
Verfügbarkeit **(Art. 32 (1) b) DSGVO)**	• Wirecard betreibt zwei Rechenzentren an verschiedenen Standorten, die gemäß den BSI-Anforderungen mindestens 5 km voneinander entfernt liegen, um ein hohes Maß an Betriebssicherheit zu gewährleisten. In jedem Rechenzentrum ist Redundanz für alle wichtigen Systemkomponenten eingebaut. • Die Rechenzentren richten sich nach dem TIER 3-Standard des Uptime Institutes aus und sind nach ISO 27001 oder nach ISAE 3402 zertifiziert; dadurch werden geeignete Maßnahmen zu ihrem Schutz vor Ausfällen und die darauf abgestimmten Verfahren garantiert. • Alle Daten werden in regelmäßigen Abständen (täglich) gesichert und durch strukturelle Maßnahmen getrennt an einem sicheren Ort unter Einhaltung der BSI-Anforderungen (auch in Bezug auf Sabotage) aufbewahrt. • Alle Systeme werden rund um die Uhr überwacht, so dass bei Auftreten von Fehlern sofort gehandelt werden kann. • Als Dienstleister verarbeitet Wirecard für eine Vielzahl von Kunden Daten für die Zahlungsabwicklung im Rahmen der Auftragsdatenverarbeitung. Durch die sorgfältige Vergabe von Zutrittsrechten wird sichergestellt, dass sämtliche Daten nur entsprechend der Zweckbindung und den Anweisungen des Verantwortlichen verarbeitet werden. • Alle relevanten Daten werden in den Datenbanken von Wirecard mit einer eindeutigen Kundenidentifikation gespeichert, so dass eine eindeutige Zuordnung jederzeit möglich ist. Gleichzeitig werden Testdaten klar von jeglichen Produktionsdaten getrennt. • Darüber hinaus wird die strikte Zweckbindung und Trennung der Verarbeitung durch regelmäßige Schulungen der Mitarbeiter sowie durch regelmäßig durchgeführte Überprüfungen der IT-Sicherheit gewährleistet.

Belastbarkeit von Verarbeitungssystemen (Art. 32 (1) b) DSGVO)	• Eine Sicherheitsbewertung der Netzwerkkonfiguration und des Firewall-Regelwerks erfolgt zweimal im Jahr, wobei Schwachstellenscans/-bewertungen alle 90 Tage und Penetrationstests mindestens einmal im Jahr durchgeführt und gemäß den PCI-DSS-Vorschriften auf Anwendungs- und Netzwerkebene implementiert werden. • Wirecard betreibt sowohl Intrusion Detection Systeme (IDS) als auch Intrusion Protection Systeme (IPS), wobei ein rund um die Uhr arbeitender Bereitschaftsdienst im Falle eines Ausfalls (Zwischenfalls) für zeitnahe Alarmierungen sorgt. • Auf allen Arbeitsplatzrechnern sind Antivirenlösungen installiert, die automatisch und kontinuierlich aktualisiert werden. Mobile Computer (Laptops) sind mit Festplattenverschlüsselung ausgestattet.
Verfahren zur Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls (Art. 32 (1) c) DSGVO)	• Backup-Pläne, die den Anforderungen der bei Wirecard gehosteten Systeme entsprechen, wurden eingerichtet. Zur Automatisierung des Backup-Vorgangs wird eine Networker-Appliance verwendet. • Standard-Clients werden täglich durch ein differenzielles/inkrementelles Backup gesichert und es werden wöchentlich komplette Backups durchgeführt. • Die Datenbanken in den Hauptrechenzentren werden in das Nebenrechenzentrum dupliziert. Daher ist für die in der Datenbank gespeicherten Informationen kein regelmäßiges externes Backup notwendig. Ein komplettes Backup der Daten erfolgt zweimal wöchentlich und es wird täglich ein differenzielles Backup durchgeführt. • Die Dateisystemsicherung des Datenbankservers erfolgt einmal pro Woche und täglich (differentiell). Diese Sicherungen werden als lokales Backup auf Band durchgeführt. • Alle Backups sind gemäß Anforderungen in Bezug auf Compliance, geschäftliche und gesetzliche Anforderungen aufbewahrungspflichtig. • Alle Sicherungsbänder werden für einen festgelegten Zeitraum (Aufbewahrungsdauer) gemäß den Unternehmensrichtlinien gespeichert. • Appliances und Server, die VMWare verwenden, werden durch Snapshots des Systems gesichert. • Alle sechs Monate werden Readiness Tests zur Datensicherung und -wiederherstellung durchgeführt. Darüber hinaus werden nach jeder Änderung der Backup-Infrastruktur und der Backup-Umgebung Tests durchgeführt. • Wirecard plant das Business Continuity und das IT Disaster Management auf Basis des allgemeinen Risiko- und IT-Risikomanagementverfahrens sowie der zugrundeliegenden Business-Impact-Analyse. Das Gesamtkonzept des Infrastrukturaufbaus und der Online-Verarbeitungssysteme folgt einem Aufbau mit hoher Verfügbarkeit und Belastbarkeit durch Clustering und Redundanzmechanismen sowohl auf Hardware- als auch auf Anwendungsebene.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 (1) d) DSGVO)	• Einzelne Geschäftsbereiche der Wirecard werden mindestens einmal im Jahr durch die BaFin überprüft. • Wirecard ist ein PCI DSS-konformes Unternehmen, das jedes Jahr von qualifizierten Sicherheitsgutachtern (Qualified Security Assessors, QSA) nach den Anforderungen des PCI DSS bewertet wird. • Die Systeme von Wirecard werden mindestens vierteljährlich Schwachstellenanalysen durch interne Sicherheitsanalytiker unterzogen. Die Scans werden an all unseren Produktionslösungen durchgeführt, um eine effiziente Überprüfung bekannter Risiken zu gewährleisten. • Externe Schwachstellenbewertungen werden vierteljährlich von einem Approved Scanning Vendor (ASV) durchgeführt, um sicherzustellen, dass unsere externen Lösungen weiterhin den PCI-DSS-Anforderungen entsprechen; diese Scans werden von unserer PCI-Prüfungsgesellschaft durchgeführt. • Penetrationstests auf Netzwerk- und Anwendungsebene werden auf den Systemen von Wirecard mindestens jährlich oder bei wesentlichen Änderungen durchgeführt. Tests werden intern und extern durchgeführt. • Zusätzlich zu den vorstehend genannten Tests werden mindestens vierteljährlich Scans nach nicht autorisierten Wireless Access Points durchgeführt. Dieses Verfahren muss von einer geschulten Person des IT-Sicherheitsteams durchgeführt werden. Der Scan wird an allen Standorten, einschließlich der Rechenzentren und Büroräumlichkeiten durchgeführt.