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 „DSGVO“) 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 Vereinb arung 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 DSGVO 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 DSGVO 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) DSGVO 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 DSGVO sowie über gerichtliche Entscheidungen im Zusammenhang mit den Art. 83, 84 DSGVO 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 DSGVO

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 DSGVO 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. Folgender Unterauftragnehmer ist zum Zeitpunkt des Vertragsschlusses mit der Erbringung von vertragsrelevanten Leistungen beauftragt:

   - als IT-Dienstleister die Akra GmbH, die neben Wartungstätigkeiten auch Hosting- und Serverleistungen erbringt;

   - Hermes Germany GmbH für die Erstellung eines Versandlabels.

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 DSGVO, 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 seiner Wahl 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.w

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

ANLAGE 1

TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHME

ALLGEMEIN

Datensicherheit und Datenschutz sind wichtige Grundsätze der Verarbeitung von Daten bei Wirecard. Wirecard ist sich bewusst, dass sie eine große Menge sensibler und personenbezogener Daten verarbeitet und diese Daten als eines ihrer wichtigsten Güter besonders schützen muss Wirecard versichert hiermit die Einhaltung aller datenschutzrechtlichen Vorgaben im Rahmen der Auftragsdatenverarbeitung, insbesondere der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Alle Mitarbeiter der Wirecard sind auf die Einhaltung des Datengeheimnisses gemäß Art. 28 Abs. 3b) DSGVO verpflichtet. Es existiert ein öffentliches Verfahrensverzeichnis, das auf Anfrage zur Verfügung gestellt werden kann, sowie ein internes Verarbeitungsverzeichnis zur Prüfung der datenschutzrelevanten Anwendungen.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die DSGVO definiert verschiedene technische und organisatorische Maßnahmen, die für eine ordnungsgemäße Verarbeitung von personenbezogenen Daten getroffen werden müssen. Dabei handelt es sich im Einzelnen um folgende Punkte.

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennung der Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten

Die für die Einhaltung der einzelnen Punkte ergriffenen Maßnahmen werden im Folgenden genauer erläutert.

ZUTRITTSKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren."

Alle Räumlichkeiten der Wirecard verfügen über ein chipkartenbasiertes Zutrittssystem. Zugänge zu verschiedenen Bereichen innerhalb der Gebäude werden dabei unterschieden. Allen Mitarbeitern werden Chipkarten mit den für ihre Arbeit erforderlichen Zutrittsrechten ausgegeben. Die zentral vom Bereich Facility Management erteilten Zutrittsrechte werden dokumentiert und in regelmäßigen Abständen vom Bereich IT Security überprüft. Besucher dürfen sich in den Büros nur in Begleitung bewegen und erhalten gesonderte Ausweise. Alle Zugänge zu den Gebäuden von Wirecard werden videoüberwacht. Der Zugang zu den Rechenzentren ist streng reglementiert. Jeder Zutritt zu den Rechenzentren bedarf einer gesonderten Anmeldung, dies gilt auch für Wirecard Mitarbeiter. Die Anmeldungen erfolgen fälschungssicher (authentifiziert) durch Abteilungsleiter der IT. Dritte dürfen nur in Ausnahmefällen und in Begleitung von Wirecard Mitarbeitern die Rechenzentren betreten. Jeder Zugang wird revisionssicher protokolliert. Die Zugangsprotokolle werden regelmäßig durch den Bereich IT Security überprüft. Die Rechenzentren sind gegen unbefugten Zutritt durch Wachpersonal, das rund um die Uhr vor Ort ist, sowie Videoüberwachung und Alarmanlagen geschützt.

Referenzdokumente:
IT Security Policy, Physical Access Restrictions Policy

ZUGANGSKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können."

Sämtliche Systeme bei Wirecard sind mit Zugangskontrollsystemen ausgestattet. Jeder Mitarbeiter bei Wirecard verfügt über persönliche Zugang zu den Systemen, die jeweils mit nur ihm bekannten, persönlichen Passworten gesichert sind. Die Passwort-Richtlinien verlangen eine regelmäßige Veränderung des persönlichen Passworts (systemabhängig sind Zeiträume von 90 Tagen oder kürzer konfiguriert) und stellen die Qualität bzw. Komplexität des Passworts anhand von definierten Regeln sicher. Alle Regeln zur Passwortvergabe und -änderung sind schriftlich fixiert. Die Bildschirme aller Arbeitsstationen und alle Services, die personenbezogene Daten verarbeiten oder speichern werden automatisch nach 15 Minuten Inaktivität gesperrt. Ein Entsperren ist nur mit dem persönlichen Benutzerpasswort durch wiederholten Log-In möglich. Die Sperrung des Arbeitsplatzrechners bei Verlassen des Arbeitsplatzes ist zudem durch eine interne Richtlinie verbindlich geregelt.

Referenzdokumente:
IT Security Policy, IT Access Control Policy, Remote Access Policy, Password Creation Guidelines, Data Classification and Control Policy, Personnel Facing Technologies Usage Policy, Security Awareness and Acceptable Usage Policy, Logging Controls Policy, Data Classification and Control Policy

---

ZUGRIFFSKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können."

Der Zugriffskontrolle liegt ein Rollen- und Rechtesystem zugrunde, mit dem das Need-to-Know Prinzip des Datenzugriffs sichergestellt wird. Somit hat jeder Mitarbeiter Zugriff auf genau die Daten, die er für seine tägliche Arbeit benötigt. Die für die jeweilige Stelle des Mitarbeiters notwendigen Rechte sind als Rollen definiert, die dem Mitarbeiter zugewiesen werden. Darüber hinausgehende Einzelberechtigungen müssen vom Bereich IT Security freigegeben werden. Die Freigabe erfolgt nach Rücksprache mit dem Information Owner (i.d.R. der Leiter der zuständigen Fachabteilung) und im Rahmen der datenschutzrechtlichen Instruktionen. Die Rechtevergabe wird nachvollziehbar dokumentiert. Die Rollenbeschreibungen und vergebenen Rechte werden von den zuständigen Abteilungen dokumentiert und gepflegt und in regelmäßigen Abständen (mind. einmal jährlich) vom Bereich IT Security stichprobenartig überprüft. Administratorzugänge werden nur nach vorheriger interner Schulung vergeben. Sämtliche Administratorzugriffe auf die Systeme werden revisionssicher protokolliert. Die Verhinderung des unbefugten Zugriffs auf Daten wird durch das regelmäßige und zeitnahe Einspielen von Sicherheitsupdates für alle genutzten Drittapplikationen gewährleistet, die IT Betriebssysteme (OS) werden monatlich mit Sicherheitsupdates versorgt. Die Qualität eigenentwickelter Applikationen wird vor Inbetriebnahme durch einen umfangreichen Qualitätssicherungsprozess sichergestellt. Die Systeme von Wirecard sind über ein mehrstufiges Firewall-Konzept gegenüber dem Internet abgesichert. Alle Änderungen in den Firewalls unterliegen einem internen Freigabeprozess und werden vom Bereich IT Security geprüft. Die Netzwerkkonfiguration und die aus dem Internet erreichbaren Payment-Applikationen werden zudem in den mindestens einmal jährlich von Netzwerk- und Vulnerability- Scans überprüft.

Wirecard betreibt Intrusion Detection Systeme (IDS) und Intrusion Protection Systeme (IPS) und gewährleistet durch 24/7 Bereitschaft eine zeitnahe Alarmierung bei Störungen (Incidents). Alle Arbeitsplatzrechner sind mit einem Virenschutz ausgestattet, der automatisch laufend aktualisiert wird. Mobile Rechner (Laptops) sind mit einer Festplattenverschlüsselung ausgestattet.

Referenzdokumente:
IT Security Policy, IT Access Control Policy, IT and Information Security Policy, Data Classification and Control Policy, Security Awareness and Acceptable Usage Policy, Security Incident Response Plan and Procedures Policy, Incident Management from Sharepoint, Logging Controls Policy, Roles and Responsibilities Policy, Firewall Security Administration Policy, Anti-Virus Policy

---

WEITERGABEKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.“

Der Austausch und die Übertragung personenbezogener Daten erfolgt grundsätzlich nur in verschlüsselter Form. Abhängig von der Art der Weitergabe werden SSL-verschlüsselte Übermittlungsverfahren über HTTPS und SFTP verwendet. E-Mails und Dateien können verschlüsselt werden (z.B. PGP-Verschlüsselung für regelmäßigen, verschlüsselten Datenaustausch). Zusätzlich existiert ein System zum sicheren einmaligen Versand von personenbezogenen Daten (Prinzip des Datenraumes). Verschlüsselung beim Austausch personenbezogener Daten ist ein zentrales Thema der allgemeinen Datenschutzschulungen, die für jeden Mitarbeiter verpflichtend sind. Alle Schnittstellen zu externen Stellen, über die personenbezogene Daten automatisiert übertragen werden, sind nach aktuellen Standards gesichert, z.B. durch SSL Verschlüsselung. Sämtliche Schnittstellen sind dokumentiert. Die externen Dokumentationen der Schnittstellen liegen vor. Media Inventories und eine Clean Desk Policy verhindern die Unberechtigte Einsicht und den Diebstahl von Datenträgern und Unterlagen. Datenträger oder Unterlagen mit besonderen personenbezogenen Daten werden grundsätzlich per Kurier versandt, die Datenträger werden verschlüsselt.

Referenzdokumente:
IT Security Policy, IT and Information Security Policy, Encryption Policy, Logging Controls Policy, Media Policy

---

EINGABEKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind."

Bei Administratorzugriffen werden alle Änderungen an personenbezogenen Daten in den Systemen der Wirecard durch die jeweilige Software-Applikation protokolliert oder durch entsprechende Prozesse dokumentiert, so dass sämtliche Änderungen jederzeit nachvollzogen werden können. Jeder Mitarbeiter hat zum Zwecke der Dateneingabe und -änderung eine persönliche Nutzerkennung für das jeweilige System, so dass alle Eingaben einer Person zugeordnet werden können.

Referenzdokumente:
IT Security Policy, IT Access Control Policy, Logging Controls Policy, Data Retention and Disposal Policy

---

AUFTRAGSKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können."

Wirecard stellt als Auftragnehmer bereits durch die Regelungen im Vertrag mit dem jeweiligen Auftraggeber individuell sicher, dass die rechtlichen Grundlagen der Auftragsdatenverarbeitung beachtet werden. Die Regelungen entsprechen den Vorgaben des Art. 28 DSGVO. Wirecard achtet ebenfalls bei der Vergabe von Aufträgen zur Auftragsdatenverarbeitung besonders auf die Einhaltung der datenschutzrechtlichen Vorschriften. Vor der Vergabe von Aufträgen werden Auftragnehmer ordnungsgemäß überprüft im Hinblick auf technische, finanzielle, datensicherheitsspezifische und rechtliche Aspekte. Die Überprüfung beinhaltet einen Ortsbesuch, Gespräche mit den Repräsentanten des Unternehmens und Hintergrundchecks über öffentlich zugängliche Quellen. Alle vertraglichen Regelungen werden vom Datenschutzbeauftragten bzgl. der Konformität mit der DSGVO geprüft. Alle Mitarbeiter im Hause Wirecard werden regelmäßig zu den aktuellen Regelungen des Datenschutzes geschult. Zudem werden alle Mitarbeiter bei ihrer Einstellung auf das Datengeheimnis gemäß Art. 28 Abs. 3b) DSGVO verpflichtet.

Referenzdokumente:
IT Security Policy, IT and Information Security Policy, Third Parties and Third Party Agreements Policy, Personnel Facing Technologies Usage Policy, Security Awareness and Acceptable Usage Policy

---

VERFÜGBARKEITSKONTROLLE

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind."

Wirecard betreibt zwei Rechenzentren an unterschiedlichen Standorten die gemäß den Vorgaben BSI mindestens 5 km voneinander entfernt sind, um ein Höchstmaß an Ausfallsicherheit zu gewährleisten.

Innerhalb jedes Rechenzentrums sind alle wichtigen Systemkomponenten redundant ausgelegt. Die Rechenzentren entsprechen mindestens dem Standard TIER 3 des Uptime Institutes und haben eine ISO 27001 oder ISAE 3402 Zertifizierung, das garantiert angemessene Maßnahmen zur Sicherung vor Ausfällen und darauf abgestimmte Prozesse. Backups aller Daten werden regelmäßig (täglich) angefertigt und an einem sicheren, durch bauliche Maßnahmen getrennten Ort aufbewahrt, dabei werden die Vorgaben des BSI (auch bezüglich Sabotage) befolgt. Alle Systeme werden rund um die Uhr überwacht, so dass im Fehlerfall umgehend reagiert werden kann.

Referenzdokumente:
IT Security Policy, Backup Policy, Backup and Availability Policy

TRENNUNG DER VERARBEITUNG VON ZU UNTERSCHIEDLICHEN ZWECKEN ERHOBENEN DATEN

„ sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrenntverarbeitet werden können.“

Wirecard verarbeitet als Dienstleister für Zahlungsabwicklung im Rahmen der Auftragsdatenverarbeitung Daten für eine große Menge von Kunden. Dabei wird durch die sorgfältige Vergabe der Zugriffsrechte sichergestellt, dass alle Daten nur gemäß ihrer Zweckbindung und den Weisungen des Auftraggebers entsprechend verarbeitet werden. Alle relevanten Daten werden in den Datenbanken von Wirecard unter Angabe einer eindeutigen Mandantenkennung gespeichert, so dass eine eindeutige Zuordnung jederzeit möglich ist, Testdaten sind dabei eindeutig von produktiven Daten getrennt. Die strikte Zweckbindung und Trennung der Verarbeitung wird zudem durch regelmäßige Schulung der Mitarbeiter sowie durch regelmäßige Prüfungen durch den Bereich Informationssicherheit sichergestellt.

Referenzdokumente:
IT Security Policy, IT and Information Security Policy, Data Classification and Control Policy