PAYREXX AG
Burgstraße 20
CH-3600 Thun

Auftragsvearbeitungsvertrag

zwischen

Sienna Finanzen GmbH
Zusatz
Unterdorf 21
7027 Lüen

Kundin

und

Payrexx AG

Burgstrasse 20, 3600 Thun, Schweiz

Anbieterin

(Kundin und Anbieterin je einzeln eine "Partei" und zusammen die "Parteien")

A. Allgemeine Bestimmungen

1. Gegenstand und Anwendungsbereich dieser Vereinbarung

1.1. Diese Vereinbarung über die Auftragsbearbeitung ("**Vereinbarung**") konkretisiert die Rechte und Pflichten der Parteien in Bezug auf die Auftragsbearbeitung, die sich für sie aus dem anwendbaren Datenschutzrecht ergeben. Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen zwischen den Parteien. Dabei kann es sich um einen einzelnen oder mehrere Verträge zwischen den Parteien über die Leistungserbringung für die Kundin handeln ("**Vertrag**").

1.2. Die Vereinbarung gilt nur in Bezug auf Dienstleistungen, bei denen die Anbieterin Personendaten im Auftrag und für Zwecke der Kundin bearbeitet ("**Auftragsbearbeitung**"), wobei die Kundin entweder Verantwortliche oder Auftragsbearbeiterin und die Anbieterin entweder Auftragsbearbeiterin oder Unter-Auftragsbearbeiterin ist.

1.3. Diese Vereinbarung gilt ausdrücklich nicht für Bearbeitungen von Personendaten, bei denen die Anbieterin die Zwecke und Mittel der Bearbeitung bestimmt und somit unter anwendbaren Datenschutzgesetzen für die Datenbearbeitung verantwortlich ist.

1.4. Diese Vereinbarung wird mit ihrer gegenseitigen Unterzeichnung durch die Parteien verbindlich.

1.5. Diese Vereinbarung ist ein integraler Bestandteil des Vertrags. Die Bestimmungen dieser Vereinbarung schränken die Rechte und Pflichten der Parteien in Bezug auf die Erbringung von Dienstleistungen unter dem Vertrag nicht ein. Ihren Regelungsgegenstand betreffend gehen die Bestimmungen dieser Vereinbarung indes den Bestimmungen des Vertrags vor.

2. Laufzeit der Vereinbarung

2.1. Die Laufzeit dieser Vereinbarung entspricht der Dauer des Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung keine zeitlich darüber hinausgehenden Verpflichtungen ergeben. Bei solchen überdauernden Verpflichtungen besteht diese Vereinbarung solange fort, bis die entsprechenden Verpflichtungen erloschen sind.

2.2. Durch diese Regelung modifizieren die Parteien nicht die im Vertrag vereinbarten Kündigungsrechte.

3. Definitionen

3.1. Die in dieser Vereinbarung in Fettschrift hervorgehobenen und in Anführungs- und Schlusszeichen gesetzten Begriffe haben in der gesamten Vereinbarung die ihnen darin zugeschriebene Bedeutung.

3.2. Die in dieser Vereinbarung verwendeten datenschutzbezogenen Begriffe wie "Personendaten" (personenbezogene Daten), "betroffene Person" , "Verantwortlicher", "Auftragsbearbeiter", oder "Datenschutz-Folgenabschätzung" haben die ihnen im Schweizer Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG) bzw. (wo anwendbar) in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (EU-DSGVO) zugeschriebene Bedeutung.

B. Beschreibung der Auftragsbearbeitung und Pflichten der Parteien

4. Angaben zur Auftragsbearbeitung und Zweck

4.1. Gegenstand und Zweck der Auftragsbearbeitung ergeben sich aus dem Vertrag und den Leistungsbeschreibungen der Anbieterin in Verbindung mit allfälligen separaten Weisungen der Kundin.

4.2. Die Art der Bearbeitung, die Art der bearbeiteten Personendaten ("**vertragsgegenständliche Personendaten**") und der Kreis (Kategorien) betroffener Personen bestimmen sich ebenfalls nach dem Vertrag und den Leistungsbeschreibungen der Anbieterin in Verbindung mit allfälligen separaten Weisungen der Kundin.

4.3. Die Auftragsbearbeitung erfolgt in der Schweiz, den Vereinigten Staaten, Irland und Malta, wobei die Anbieterin die datenschutzrechtliche Zulässigkeit der Weiterübermittlung an Unter-Auftragsbearbeiter in Staaten ohne angemessenes Datenschutzniveau durch Abschluss von EU Standardvertragsklauseln (Modul 3) sicherstellt.

4.4. Die Dauer der Bearbeitung bestimmt sich nach Ziffer 2.

5. Weisungsgebundenheit, Zweckbindung und Kontrolle

Die Anbieterin verpflichtet sich und sichert zu, dass die Anbieterin alle

vertragsgegenständlichen Personendaten (i) ausschliesslich zu den in Ziffer 4 beschriebenen Zwecken, (ii) in Übereinstimmung mit den Weisungen der Kundin sowie (iii) in Übereinstimmung mit dieser Vereinbarung bearbeitet; und (iv) nicht für eigene Zwecke verwendet.

6. Datensicherheit

6.1. Die Anbieterin verpflichtet sich, im Interesse der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit der vertragsgegenständlichen Personendaten angemessene technische und organisatorische Schutzmassnahmen zu treffen.

6.2. Die Anbieterin implementiert hierzu insbesondere Zugangskontrollen, Zugriffskontrollen sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen. Bei der Auswahl der Massnahmen berücksichtigt die Anbieterin den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für betroffene Personen.

7. Meldung von Verletzungen der Datensicherheit

7.1. Wenn die Anbieterin eine Verletzung der Sicherheit bemerkt, die darin besteht, dass vertragsgegenständliche Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden ("**Verletzung der Datensicherheit**"), wird die Anbieterin die Verletzung der Datensicherheit so rasch als möglich und ohne schuldhaftes Zögern der Kundin melden. Die Anbieterin wird die Verletzung der Datensicherheit sodann (i) untersuchen und die Auswirkungen ermitteln, (ii) die Kundin detailliert über die Verletzung der Datensicherheit informieren und (iii) angemessene Massnahmen ergreifen, um die Auswirkungen zu mildern und das Risiko, das sich aus der Verletzung der Datensicherheit für betroffene Personen möglicherweise ergibt, so gering wie möglich zu halten.

7.2. Die Anbieterin wird die Kundin in angemessener Weise unterstützen, um die Kundin bei der Erfüllung ihrer Verpflichtungen zu unterstützen, Verletzungen der Datensicherheit an zuständige Aufsichtsbehörden oder an betroffene Personen zu melden.

8. Informations- und Unterstützungspflichten

8.1. Die Anbieterin verpflichtet sich, die Kundin so rasch wie möglich und von sich aus zu informieren, (i) wenn die Anbieterin der Ansicht ist, dass die Anbieterin in absehbarer Zeit nicht mehr in der Lage ist, den Pflichten gemäss dieser Vereinbarung nachzukommen; sowie (ii) über jede Anfrage zur Ausübung von Betroffenenrechten, welche die Anbieterin direkt von betroffenen Personen in Bezug auf vertragsgegenständliche Personendaten erhalten hat (vorausgesetzt, die Anbieterin kann eine Zuordnung an die betroffene Person gestützt auf die

Angaben der betroffenen Person vornehmen; andernfalls wird die Anbieterin die betroffene Person bitten, sich an die für die Datenbearbeitung Verantwortliche zu wenden).

8.2. Die Anbieterin verpflichtet sich, die Kundin auf Anfrage und gegen separate Vergütung bei der Beantwortung von Anfragen betroffener Personen zur Ausübung datenschutzrechtlicher Betroffenenrechte zu unterstützen.

8.3. Zudem verpflichtet sich die Anbieterin, die Kundin auf Anfrage und gegen separate

Vergütung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen von Datenschutzaufsichtsbehörden zu unterstützen.

8.4. Die Anbieterin stellt der Kundin alle Informationen zur Verfügung, welche die Kundin vernünftigerweise für den Nachweis der Einhaltung ihrer Verpflichtungen aus dem anwendbaren Datenschutzrecht in Bezug auf die Auftragsbearbeitung benötigt. Auf Anfrage der Kundin stellt die Anbieterin zudem allfällige Berichte zur Informationssicherheit bereit, die eine Prüfgesellschaft oder Zertifizierungsstelle in Bezug auf die Dienstleistungen der Anbieterin oder ihrer Unter-Auftragsbearbeiter erstellt hat.

9. Geheimhaltung

9.1. Die Anbieterin verpflichtet sich zur Geheimhaltung der vertragsgegenständlichen Personendaten und hat die mit der Auftragsbearbeitung betrauten Personen zur Wahrung der Vertraulichkeit zu verpflichten.

9.2. Diese Geheimhaltungsverpflichtungen gelten auch nach Beendigung dieser Vereinbarung für unbeschränkte Dauer weiter.

10. Unter-Auftragsbearbeiter

10.1. Unter-Auftragsbearbeiter sind natürliche oder juristische Personen, welche die Anbieterin für die Auftragsbearbeitung beizieht. Die Anbieterin ist berechtigt, Unter-Auftragsbearbeiter beizuziehen. Die Anbieterin ist in solchen Fällen verpflichtet, mit Unter-Auftragsbearbeitern im erforderlichen Umfang eine Vereinbarung über die (Unter-)Auftragsbearbeitung zu treffen, die der Anbieterin die Einhaltung der Bestimmungen der vorliegenden Vereinbarung zwischen der Anbieterin und der Kundin ermöglicht. Dies beinhaltet auch die Überbindung der Geheimhaltungspflichten der Anbieterin auf den Unter-Auftragsbearbeiter.

10.2. Die Anbieterin wird die Kundin vorab in geeigneter Weise schriftlich informieren, wenn die Anbieterin nach Inkrafttreten dieser Vereinbarung beabsichtigt, neue Unter-Auftragsbearbeiter beizuziehen oder bestehende auszutauschen. Wenn die Kundin dem Beizug bzw. Austausch des Unter-Auftragsbearbeiters nicht innerhalb von dreissig (30) Tagen nach dem Datum der Mitteilung schriftlich widerspricht, gilt der neue oder ausgetauschte Unter-Auftragsbearbeiter als genehmigt.

10.3. Die Kundin hat einen allfälligen Widerspruch gegen den neuen oder ausgetauschten Unter-Auftragsbearbeiter zu begründen. Erfolgt der Widerspruch aus zwingenden gesetzlichen oder regulatorischen Gründen, so kann die Anbieterin wahlweise einen anderen Unter-Auftragsbearbeiter beiziehen oder der Kundin ein ausserordentliches Kündigungsrecht gewähren. Erfolgt der Widerspruch nicht aus gesetzlich oder regulatorisch zwingenden Gründen und hält die Anbieterin am Unter-Auftragsbearbeiter fest, so initiiert die Anbieterin einen Einigungsversuch mit der Kundin, zu dem die Anbieterin weitere Parteien (namentlich andere Kundinnen der Anbieterin und den Unter-Auftragsbearbeiter) beiziehen kann. Scheitert der Einigungsversuch, steht es der Kundin frei, auf die Nutzung der Dienstleistungen zu verzichten und den Vertrag ausserordentlich zu kündigen.

11. Rückgabe oder Löschung vertragsgegenständlicher Personendaten bei Vertragsbeendigung

Im Falle einer Registrierung bei Payrexx mit anschließender Know-Your-Customer-Überprüfung (KYC) wird die Anbieterin die Geschäftskorrespondenz samt vertragsgegenständlichen Personendaten nach Beendigung des Vertrags nach Artikel 957 und 963 des Schweizer Obligationenrechts für eine Dauer von zehn Jahren archivieren. Sofern die Kundin das KYC nicht

abgeschlossen hat, wird die Anbieterin die Daten sofort löschen.

12. Audit

12.1. Die Kundin kann bei der Anbieterin einmal jährlich ein Audit zur Prüfung der Sicherheitsmassnahmen oder der sonstigen Einhaltung dieser Vereinbarung durchführen oder durchführen lassen. Die Kosten dafür trägt die Kundin. Die Anbieterin unterstützt die Audits im Rahmen eines verhältnismässigen Aufwands unentgeltlich.

12.2. Die Prüfungs- und Auditrechte gemäss dieser Vereinbarung gelten nur insoweit als der Vertrag der Kundin nicht anderweitig erlaubt, die Erfüllung dieser Vereinbarung durch die Anbieterin zu prüfen und zu auditieren.

PAYREXX AG
Burgstraße 20
CH-3600 Thun

Für Kundin:

Unterschrift: ..... Signiert von: Nando scherrer EE7B42546F1A4A8... Unterschrift: .....

Name: Nando scherrer ..... Name: .....

Datum: 11/23/2025 ..... Datum: .....

Für Payrexx AG:

Unterschrift: ..... DocuSigned by: Ivan Schmid D8C6181207 9C405... Unterschrift: ..... DocuSigned by: Ueli Kramer 0FE1D3209BB34C2...

Name: Ivan Schmid Name: Ueli Kramer

Datum: 11/23/2025 ..... Datum: 11/23/2025 .....

PAYREXX AG
Burgstraße 20
CH-3600 Thun

Anlage 1

Aktuelle Unter-Auftragsbearbeiter

Serverumgebung

Amazon Web Services (AWS)
Serverstandort: Deutschland (Frankfurt)
Datenschutzrichtlinien: https://aws.amazon.com/de/privacy

Kundenverwaltung

Google Suite
Serverstandort: Weltweit
Datenschutzrichtlinien: https://policies.google.com/privacy

Bexio
Serverstandort: Schweiz
Datenschutzrichtlinien: https://www.bexio.com/de-CH/richtlinien/datenschutz

Hubspot
Serverstandort: Deutschland (AWS)
Datenschutzrichtlinien: https://legal.hubspot.com/privacy-policy

Flow Swiss
Serverstandort: Schweiz
Datenschutzrichtlinien: https://flow.swiss/privacy-policy/

E-Mail-Services

Mailgun
Serverstandort: EU (AWS)
Datenschutzrichtlinien: https://www.mailgun.com/privacy-policy

SendGrid
Serverstandort: USA
Datenschutzrichtlinien: https://sendgrid.com/policies/privacy/services-privacy-policy

MailChimp
Serverstandort: USA
Datenschutzrichtlinien: https://mailchimp.com/legal/privacy

SMS-Services

Twilio
Serverstandort: Deutschland (Frankfurt, AWS)
Datenschutzrichtlinien: https://www.twilio.com/legal/privacy

PAYREXX AG
Burgstraße 20
CH-3600 Thun

Angebundene Zahlungsanbieter

Anbieter	Hauptsitz	Datenschutzrichtlinien
PostFinance	Schweiz	https://www.postfinance.ch/privacyapp
PayPal	USA	https://www.paypal.com/ch/webapps/mpp/ua/privacy-full
PAYMILL	Deutschland	https://www.paymill.com/de/datenschutz
Stripe	Irland	https://stripe.com/ch/privacy
Ingenico	Deutschland	https://ingenico.de/payment-services/service/datenschutz
Giropay	Deutschland	https://www.giropay.de/rechtliches/datenschutzerklaerung
Concardis	Deutschland	https://www.concardis.com/ch-de/datenschutz
Braintree	USA	https://www.braintreepayments.com/en-ch/legal
Sofort	Deutschland	https://www.klarna.com/sofort/datenschutz
BillPay	Deutschland	https://www.billpay.ch/de/datenschutz-ch
Twint	Schweiz	https://www.twint.ch/datenschutz-website
Saferpay - SIX	Schweiz	https://www.six-payment-services.com/de/services/legal/privacy-statement.html
Datatrans	Schweiz	https://www.datatrans.ch/de/datenschutzbestimmungen
VIVEUM	Österreich	https://www.viveum.com/datenschutzerklaerung
SWISSBILLING	Schweiz	https://www.swissbilling.ch/datenschutz
BS PAYONE	Deutschland	https://www.bspayone.com/DE/de/privacy
WIRpay	Schweiz	https://www.wir.ch/rechtliche-hinweise
Mollie	Niederlande	https://www.mollie.com/de/privacy
Skrill	Vereinigtes Königreich	https://www.skrill.com/de/fusszeile/datenschutzrichtlinie
VR pay	Deutschland	https://www.vr-pay.de/datenschutz-haftung
WorldPay	Vereinigtes Königreich	https://www.worldpay.com/uk/privacy-policy

PAYREXX AG
Burgstraße 20
CH-3600 Thun

CCAvenue	Indien	https://www.ccavenue.com/privacy.jsp
Razorpay	Indien	https://razorpay.com/privacy
Paysafecash	Vereinigtes Königreich	https://www.paysafecash.com/de-ch/datenschutz
PointsPay	Schweiz	https://www.pointspay.com/index.php/checkout-privacy
UTRUST	Schweiz	https://utrust.com/privacy-policy
AmazonPay	USA	https://pay.amazon.de/help/201212490
Clearhaus	Dänemark	https://www.clearhaus.com/privacy
GeckoCard	Schweiz	https://geckocard.com/de-ch/datenschutzerklaerung/
bob invoice	Schweiz	https://bob.ch/de/datenschutz
PayGate	Südafrika	https://www.paygate.co.za/gdpr
Viacash	Deutschland	https://www.viacash.com/privacy/?lang=de
OnlineÜberweisen	Deutschland	https://onlineueberweisen.com/datenschutz
Ideal Payment	Schweiz	https://www.ideal-payment.ch/impressum-datenschutz
uConekt	Schweiz	https://uconekt-pay.com/index.php/privacy/
NETS Easy	Dänemark	https://www.nets.eu/gdpr/pages/privacy-notice-for-nets.aspx
RS2	Deutschland	https://www.rs2.com/data-privacy
Credorax	Malta	https://www.credorax.com/privacy
Swisscom Pay	Schweiz	https://www.swisscom.ch/de/privatkunden/rechtliches/datenschutz/online-datenschutz.html
Visa Click-to-pay	USA	https://www.visaeurope.ch/de_CH/nutzungsbedingungen/visa-globale-datenschutzmitteilung.html

PAYREXX AG
Burgstraße 20
CH-3600 Thun

Anlage 2

Technische und organisatorische Massnahmen

1. Vertraulichkeit

1.1. Zugangskontrolle

"Unbefugten ist der (räumliche) Zutritt zu Datenverarbeitungsanlagen, in denen Kundendaten (einschliesslich Personendaten) verarbeitet werden oder genutzt werden, zu verwehren."

Umgesetzte Massnahmen:
Zutrittskontrollsystem (Ausweisleser, Magnetkarte, Chipkarte)
Multi-Faktor-Authentifizierungsverfahren
Einzelne und zeitlich begrenzte Zugangsberechtigungen
Einbruchmeldesysteme
Türsicherung (elektrische Türöffner usw.)
Werkschutz, Pförtner
Überwachungseinrichtung (Alarmanlage, Video- / Fernsehmonitor)
Protokollierung des Zutritts zum Rechenzentrum

1.2. Benutzerkontrolle

"Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können."

Umgesetzte Massnahmen:
Zutrittskontrollsystem (Ausweisleser, Magnetkarte, Chipkarte)
Multi-Faktor-Authentifizierungsverfahren
Einzelne und zeitlich begrenzte Zugangsberechtigungen
Einbruchmeldesysteme
Schlüssel / Schlüsselvergabe
Türsicherung (elektrische Türöffner usw.)
Werkschutz, Pförtner
Überwachungseinrichtung (Alarmanlage, Video- / Fernsehmonitor)
Protokollierung des Zutritts zum Rechenzentrum

1.3. Zugriffskontrolle und Speicherkontrolle

"Es ist zu gewährleisten, dass die zur Benutzung eines

Datenverarbeitungssystems Berechtigten ausschliesslich auf die zur Erfüllung ihrer Aufgaben notwendigen (Need-to Know) und ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Kundendaten (einschliesslich Personendaten) bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können."

Umgesetzte Massnahmen:
Kenntnisnahme
Anonymisierung von Daten bei Nichtnutzung
Löschung nach gesetzlicher Frist
Kein “Account-Sharing” (mehrere Personen nutzen einen Account) / eindeutige “Benutzer ID” (Benutzer-Zuordnung)

2. Integrität

2.1. Weitergabekontrolle (Transportkontrolle, Datenträgerkontrolle und Bekanntgabekontrolle)

"Es ist zu gewährleisten, dass Personendaten 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 welchen Stellen eine Übermittlung von Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist."

Umgesetzte Massnahmen:
Verschlüsselung
Protokollierung (Logging)
Transportsicherung

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle und Wiederherstellung

"Es ist zu gewährleisten, dass Kundendaten (einschliesslich Personendaten) gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind.

Rasche Wiederherstellbarkeit ist sicherzustellen."

Umgesetzte Massnahmen:
Backup-Verfahren, Widerstandsfähigkeit (Resilience) von IT-Systemen
Integrität (Integrativity) der IT-Systeme
Getrennte Aufbewahrung von KYC-Daten
Virenschutz / Firewall
Notfallplan (Disaster Recovery Plan)

3.2. Belastbarkeit und Zuverlässigkeit

"Es ist sicherzustellen, dass IT- Systeme möglichst auch bei Störungen und Fehlern funktionsfähig bleiben. Zudem ist sicherzustellen, dass Fehlfunktionen von IT Systemen intern gemeldet werden."

Umgesetzte Massnahmen:
Einrichtungen werden so geplant und implementiert, dass eine dem Risiko angemessene Ausfallsicherheit besteht.
Backup-Strategie, bei Ausfall von Datencentern

4. Verfahren zur regelmässigen Prüfung, Bewertung und Evaluierung

4.1. Datenschutzmanagement

Umgesetzte Massnahmen:
Interne Datenschutzrichtlinie
Schulungen

4.2. Incident-Response-Management (Erkennung und Minderung oder Beseitigung von Verletzungen der Datensicherheit)

Umgesetzte Massnahmen:
Incident Response-Planung
IT Reglement
Schulungen
Prozesse

4.3. Datenschutzfreundliche Voreinstellungen

Umgesetzte Massnahmen:
Grundsatz der Datenminimierung wird eingehalten
Es werden nur Daten zum Zweck gesammelt, welche in der Datenschutzerklärung angegeben werden

4.4. Auftragskontrolle

"Keine Auftragsdatenverarbeitung oder Unter-Auftragsbearbeitung ohne entsprechende Weisung des Kunden."
Umgesetzte Massnahmen:
Eindeutige Vertragsgestaltung

PAYREXX AG
Burgstraße 20
CH-3600 Thun

Schriftliche Auftragserteilung
Kriterien zur Auswahl des Auftragnehmers
Kontrolle der Vertragsausführung