PAYREXX AG
Burgstraße 20
CH-3600 Thun

Vereinbarung über die Auftragsdatenverarbeitung

Auftrag gemäß Art. 28 DS-GVO

zwischen	…… …… …… ……
im folgenden bezeichnet mit	Auftraggeber
und der Firma	**Payrexx AG** Burgstraße 20 CH-3600 Thun
im folgenden bezeichnet mit	Auftragnehmer
betreffend	Auftragsdatenverarbeitung über die Payrexx Plattform

1. Ausgangslage

Dieser Vertrag tritt - solange keine anderweitigen Regelungen vereinbart wurden - mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.
Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v. Art.4 Nr.2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen sind in Anlage 1 beschrieben.

3. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art.28 Abs.3 Satz 2 lit.c DS-GVO)

3.1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Anlage 2). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit.c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

3.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Sperrung und Löschung von Daten

4.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

5.1. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Ivan Schmid, CEO, privacy@payrexx.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

5.2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3. Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO und Anlage 2.

5.4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsdatenverarbeitung beim Auftragnehmer ermittelt.

5.6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsdatenverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

5.7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5.8. Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber, die gemäß Ziffer 3 in Anlage 2 zu entnehmen sind.

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu

gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Die Subunternehmen sind in Anlage 1 beschrieben.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch IT Sicherheits- oder Datenschutzaudit.

7.4. Der Auftraggeber verpflichtet sich, die durch eine Kontrolle verursachten und über die vereinbarte Pauschale / den vereinbarten Betrag hinausgehenden tatsächlich angefallenen Kosten zu tragen. Die Höhe der tatsächlich angefallenen höheren Kosten hat der Auftragnehmer nachzuweisen. Für die Berechnung wird der im Hauptvertrag vereinbarte Stundensatz zugrunde gelegt.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

8.1.1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

8.1.2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

8.1.3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

8.1.4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

8.1.5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstöße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

10.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

11.1. Entgelte
Ein Entgelt für diesen Auftrag wird nicht gefordert.

Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.
Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.
Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

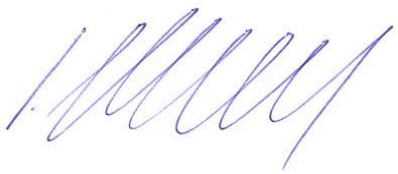
11.2. Vertragsdauer
Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung.
Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

11.3. Rechtswahl
Es gilt das Recht der Schweiz.

11.4. Gerichtsstand
Die Parteien vereinbaren als Gerichtsstand den Sitz des für Thun zuständigen Gerichts.

Unterschriften

…….., den …….. Thun, den 09.10.2019



…….. Ivan Schmid, Geschäftsführer
Auftraggeber Auftragnehmer

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

Art der Daten

Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Zahlungsdaten (Details zu getätigten Bestellungen und Zahlungen)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Auskunftsangaben (z.B. Bonitätsprüfung über Zahlungsanbieter)
- Nutzerverhalten

Kreis der Betroffenen

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter und Lieferanten des Auftraggebers

Beteiligte Subunternehmer

Hierbei handelt es sich um Dienstleister, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Payrexx verwendet eine Reihe von externen Subunternehmern, die bei der Erbringung der Hauptleistung unterstützen. Payrexx setzt nur vertrauenswürdige Subunternehmer ein:

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat. Für die in Anlage 1 aufgeführten Subunternehmer und Teilleistungen gilt diese Zustimmung als erteilt. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen Grund verweigert werden darf.
2. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
3. Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmers zu erteilen.

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

Pipedrive
Serverstandort: Deutschland (Frankfurt, AWS)
Datenschutzrichtlinien: https://www.pipedrive.com/en/privacy

E-Mail-Services

Mailgun
Serverstandort: EU
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-Service

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

Angebundene Zahlungsanbieter

Anbieter	Hauptsitz	Datenschutzrichtlinien
PostFinance	Schweiz	https://www.postfinance.ch/privacyapp
PayPal	USA	https://www.paypal.com/ch/webapps/mpp/ua/privacy-full
Stripe	USA	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
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	Irland (AWS)	https://www.clearhaus.com/privacy
AntePAY	Schweiz	https://www.antepay.com/datenschutzerklaerung
bob Finance	Schweiz	https://bob.ch/de/datenschutz
PayGate	Südafrika	https://www.paygate.co.za/gdpr

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO

Technische und organisatorische Maßnahmen gemäß Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt.

Dies umfasst die folgenden Maßnahmen:

- Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Datenzentrum durch Amazon Web Services geschützt: https://aws.amazon.com/de/compliance/data-center/controls/

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt.

Dies umfasst die folgenden Maßnahmen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Zwei-Faktor-Authentifizierung wird eingesetzt
- Automatische Sperrung (z.B. Pausenschaltung)
- Datenzentrum durch Amazon Web Services geschützt: https://aws.amazon.com/de/compliance/data-center/controls/

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt.

Dies umfasst die folgenden Maßnahmen:

- "Interne Mandantenfähigkeit" ist hergestellt
- Kontrolle der Zweckbindung
- Funktionstrennung: Production, Staging, Testing

Es findet eine Pseudonymisierung von Datensätzen statt.

Dies umfasst die folgenden Maßnahmen:

- Alle personenbezogenen Datensätze werden verschlüsselt abgespeichert.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt.

Dies umfasst die folgenden Maßnahmen:

- Sichere SSL Verbindung
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt.

Dies umfasst die folgenden Maßnahmen:

- Dokumentenmanagement, Dokumentenlenkung
- Protokollierungs- und Protokollauswertungssysteme
- Plausibilitätskontrollen
- Sicherung von Protokolldaten gegen Verlust oder Veränderung

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt.

Dies umfasst die folgenden Maßnahmen:

- Backup-Strategie
- Virenschutz / Firewall

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgenden Maßnahmen gewährleistet:

- Notfallmanagement inkl. Notfallpläne
- 24/7 Monitoring und telefonische Hotline
- Testen der Wiederherstellungssysteme

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die technischen und organisatorischen Maßnahmen wurden zuletzt an folgendem Datum evaluiert:
09.10.2019

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz.

Dies wird durch folgende Maßnahmen unterstützt:

- Regelmäßige Datenschutzschulungen

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Risikoanalyse
- Datenschutzkonzept
- Verzeichnis von Verarbeitungstätigkeiten
- Technische und organisatorische Maßnahmen
- Subunternehmer
- Auftragsdatenverarbeitungsverträge
- Datenschutzerklärung