Better Payment Germany GmbH
Rosenthaler Str. 34-35, 10178 Berlin, Germany
Tel.: +49 30 577 0101-0 , E-Mail: datenschutz@betterpayment.de

Vereinbarung zur Auftragsverarbeitung personenbezogener Daten nach Art. 28 DSGVO (AV-Vertrag)

Stand 01.03.2023

zwischen

GMC-I Service GmbH
Beuthener Straße 41
D-90471 Nürnberg

– nachfolgend der Kunde oder Auftraggeber genannt –

und

Better Payment Germany GmbH
Rosenthaler Straße 34/35
10178 Berlin
Deutschland

– nachfolgend der Better Payment oder Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3 S. 1 DSGVO)

1) Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden **Servicevertrag** (im Folgenden „Hauptvertrag").

über: **Vereinbarung der Auftragsdatenverarbeitung für die technische Abwicklung und Transmission von E-Commerce Zahlungsdaten aus Kredit- und Debit-Karten und weiteren Zahlungsarten nachfolgend "Netzbetrieb" genannt sowie die Vermittlung von Kreditkarten-Akzeptanzverträgen mit nationalen und internationalen Finanzdiensten**

2) Die Dauer dieser Vereinbarung zur Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages.

2. Gegenstand der Datenverarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

1) Die Datenverarbeitung durch den Auftragnehmer erfolgt ausschließlich zur Durchführung des Hauptvertrags.

2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

3) Im Rahmen seiner Leistungen verarbeitet der Auftragnehmer die Daten, indem er diese erhebt, erfasst, organisiert, ordnet, speichert, anpasst, verändert, ausliest, abfragt, verwendet, durch Übermittlung offenlegt, verbreitet, bereitstellt, abgleicht, verknüpft, einschränkt, löscht und/oder vernichtet.

4) Die Datenverarbeitung erfolgt ausschließlich zu den in der Leistungsbeschreibung beschriebenen Zwecken.

3. Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten

- ✓ Name, Anschrift
- ✓ Kontaktdaten (z.B. Telefon, E-Mail)
- ✓ Personendaten (z.B. Alter, Geschlecht)
- ✓ Bankdetails (z.B. Kontoinhaber, IBAN, BIC)
- ✓ Kreditkartendaten (z.B. Name, PAN, CVV, Ablaufdatum)
- ✓ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ✓ Bonitätsprüfungsdaten (z.B. Score-Bewertungen, Adressvalidierung, Identifizierung)
- ✓ Kommunikationsverbindungsdaten (z.B. Einzelverbindungsnachweis, Call Detail Records –CDR)
- ✓ Standortdaten
- ✓ IP-Adressen
- ✓ Planungs- und Steuerungsdaten
- ○ Sonstige:

_____
_____

2) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ✓ Beschäftigte
- ✓ Kunden
- ✓ Lieferanten
- ✓ Interessenten
- ✓ Abonnenten
- ✓ Handelsvertreter
- ✓ Ansprechpartner
- ○ Sonstige:

_____
_____

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

2) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

3) Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung nach Auffassung des Auftragnehmers gegen datenschutzrechtliche Vorgaben verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

4) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

7) Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt, vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

8) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort, zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu

demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

9) Der Auftragnehmer kann die Prüfung davon abhängig machen, dass die Prüfer vor der Durchführung der Kontrollen eine branchenübliche Verschwiegenheits- bzw. Vertraulichkeitserklärung abgeben oder von Gesetzes wegen zur Verschwiegenheit verpflichtet sind. Der Auftragnehmer hat in diesem Zusammenhang dazu beizutragen, dass sich der Auftraggeber oder der von dem Auftraggeber beauftragte Dritte von der Einhaltung der Pflichten des Auftragnehmers gem. Art. 28 DSGVO überzeugen kann.

10) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie in diesem Vertrag vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

5. Pflichten des Auftragnehmers

1) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

2) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

5) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten.

6) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

7) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

8) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend,

verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

9) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

10) Der Auftragnehmer hat eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz bestellt. Die Kotaktdaten des aktuellen Datenschutzbeauftragten werden in Form des Anhang 2 zu dieser Vereinbarung bereitgestellt.

6. Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 S. 2 lit. c) DSGVO)

1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen oder Sicherungen (Backups), soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

6) Die Verarbeitung von Daten außerhalb der Firmensitze des Auftragnehmers ist gestattet, sofern sichergestellt ist, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

7) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

8) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und

organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber jederzeit auf Anforderung zu überlassen. Der Nachweis kann ganz oder in Teilen durch genehmigte Verhaltensregeln oder Zertifizierungsverfahren erbracht werden.

7. Datengeheimnis (Art. 28 Abs. 3 S. 2 lit. b) DSGVO)

1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Bestimmungen bekannt sind.

2) Der Auftragnehmer gewährleistet, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis verpflichtet.

8. Unterauftragsverhältnisse / Subunternehmer (Art. 28 Abs. 2, Abs. 3 S. 21it. d), Abs. 4 DSGVO)

1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

3) Zurzeit sind die in Anhang 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

4) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

5) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

6) Eine weitere Subbeauftragung durch den Subunternehmer ist nur zulässig, wenn sämtliche Rechte und Pflichten dieser Vereinbarung mit Wirkung für den Auftraggeber auf Sub-Subunternehmer weiterübertragen werden.

7) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

8) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

9) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber auf Verlangen mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet.

10) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind aussagekräftig zu dokumentieren.

11) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

9. Betroffenenrechte (Art. 28 Abs. 3 S. 2 lit. e) DSGVO)

1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

2) Soweit eine betroffene Person sich wegen der Berichtigung, Löschung oder Einschränkung der Verarbeitung unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer hierüber den Auftraggeber informieren und das Ersuchen zeitnah an den Auftraggeber zur Erledigung weiterleiten.

3) Der Auftragnehmer unterstützt den Auftraggeber im Hinblick auf die Beantwortung von Anfragen und die Erfüllung von Ansprüchen bezogen auf die Geltendmachung von Betroffenenrechten durch betroffene Personen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann. Der Auftragnehmer erhält vom Auftraggeber eine Aufwandsentschädigung unter Berücksichtigung der vom Auftragnehmer zur Mitwirkung aufgewandten Zeit.

10. Mitteilungspflichten und Unterstützungsleistungen (Art. 28 Abs. 3 S. 21it. f) DSGVO)

1) Der Auftragnehmer unterstützt den Auftraggeber gem. Art. 32 ff. DSGVO bei der Einhaltung der Pflichten zur Sicherheit personenbezogener Daten, bei der Erfüllung von Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten, bei der Erarbeitung von Datenschutz-Folgeabschätzungen und bei der Notwendigkeit zur Durchführung von vorherigen Konsultationen.

2) Soweit der Auftragnehmer Kenntnis davon hat, dass die bei ihm getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, wird der Auftragnehmer den Auftraggeber hierüber unterrichten.

3) Der Auftragnehmer hat den Auftraggeber bei einem Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten weiter zu informieren soweit ein Bezug zu der Auftragsverarbeitung besteht oder bestehen könnte.

4) Im Falle von Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde sowie Ermittlungen der Aufsichtsbehörde wegen möglicher Ordnungswidrigkeiten und/oder Straftaten wird der Auftragnehmer ebenfalls den Auftraggeber informieren.

5) Soweit der Auftraggeber selbst einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, unterstützt ihn der Auftragnehmer in angemessenem Umfang.

6) Die vorstehenden Regelungen gelten nur unter der Voraussetzung, dass ein Bezug zum Gegenstand der Auftragsverarbeitung für den Auftraggeber besteht. Der Auftragnehmer erhält vom Auftraggeber eine Aufwandsentschädigung unter Berücksichtigung der vom Auftragnehmer aufgewandten Zeit zur Unterstützung.

11. Löschung und Rückgabe von Daten (Art. 28 Abs. 3 S. 2 lit. g) DSGVO)

1) Nach Abschluss seiner Leistungen oder früher nach Aufforderung des Auftraggebers hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- und/oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

2) Die vorstehenden Grundsätze gelten nicht für personenbezogene Daten, für die eine rechtliche Verpflichtung zur Speicherung besteht. Der Auftragnehmer hat Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Ende dieser Vereinbarung hinaus aufzubewahren; der Auftragnehmer kann sie zur eigenen Entlastung mit Ende dieser Vereinbarung an den Auftraggeber übergeben.

12. Sonstiges

1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

3) Für Nebenabreden ist die Schriftform erforderlich.

4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

5) Als Gerichtsstand wird Berlin vereinbart.

13. Unterschriften

.....	.....
Ort / Datum	Auftraggeber / Stempel
Berlin, 04.12.2023	
.....	.....
Ort / Datum	Better Payment / Stempel

Anhang 1: Technische und organisatorische Maßnahmen

Datensicherheitsmaßnahmen

der

Better Payment Germany GmbH

Die Better Payment Germany GmbH trifft folgende technische und organisatorische Maßnahmen im Sinne des Art. 32 EU DSGVO zum Schutz und zur Sicherheit von personenbezogenen Daten:

1. Zutrittskontrolle

Zielbeschreibung: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden, zu verwehren.

- Die Serverschränke im Rechenzentrum verfügen über eine Schließanlage und werden exklusiv vom Auftragnehmer genutzt.
- Elektronische Zutrittskontrollsysteme und Personal sichern und überwachen den Zutritt zum Rechenzentrum.
- Der Zutritt zum Rechenzentrum ist nur autorisierten Besuchern gestattet .
- Gelände, Gebäude und Rechenzentrumsflächen sind videoüberwacht und mit Alarmanlage gesichert.

2. Zugangskontrolle

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

- Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber genutzt und verwaltet.
- Insofern liegt es im Verantwortungsbereich des Auftraggebers, dass die eingesetzten Programme zur Datenverarbeitung nicht durch Unbefugte genutzt werden können, beispielsweise durch Verwendung einer geeigneten Passwort-Richtlinie.
- Für die Datenverarbeitungssysteme wird ein exklusiver Zugang zu einem dedizierten Bereich der Plattform zur Nutzung durch den Auftraggeber eingesetzt. Nur der Auftragnehmer zur Administration und der Auftraggeber haben Zugang zu diesem Bereich.
- Im Rahmen des Supports und der Systemwartung verfügen ausgewählte Administratoren des Auftragnehmers über privilegierten Zugriff.
- Es bestehen Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter/Schlüssel.
- Alle zugangsberechtigten Administratoren des Auftragnehmers sind auf die Einhaltung der Sicherheitsrichtlinien des Auftragnehmers und auf das Datengeheimnis verpflichtet.
- Jedem Benutzer sind Zugangsrechte zugeordnet. Diese sind auf die für die Rolle des Benutzers benötigte Rechte beschränkt.
- Authentifikation mit mindestens individueller Benutzerkennung und Passwort (je nach Systembereich sind auch strengere Zugangskontrollen wie 2-Factor-Authentication implementiert).

3. Zugriffskontrolle

Zielbeschreibung: Es ist 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

- Die erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber genutzt und verwaltet.
- Insofern liegt es im Verantwortungsbereich des Auftraggebers, dass Zugriffsberechtigungen in den eingesetzten Programmen zur Datenverarbeitung so vergeben werden, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
- Im Rahmen des Supports und der Systemwartung verfügen ausgewählte Administratoren des Auftragnehmers über privilegierten Zugriff.
- Die Anzahl der Administratoren ist auf das „Notwendigste" reduziert.
- Der Systemzugriff für Mitarbeiter oder Dienstleister des Auftraggebers ist auf das für den Betrieb notwendige Maß beschränkt.
- Alle zugangsberechtigten Administratoren des Auftragnehmers sind auf die Einhaltung der Sicherheitsrichtlinien des Auftragnehmers und auf das Datengeheimnis verpflichtet.

4. Weitergabekontrolle

Zielbeschreibung: Es ist 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.

- Die erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber genutzt und verwaltet.
- Insofern hat der Auftraggeber sicherzustellen, dass personenbezogenen Daten, die über Web-Interfaces übertragen werden, ausschließlich per SSL-Verschlüsselung (HTTPS) übertragen werden. Der Auftragnehmer unterstützt mit den geeigneten technischen Maßnahmen auf Weisung des Auftraggebers die verschlüsselte Datenübertragung per HTTPS.
- Sämtliche administrativen Aufgaben auf Systemen des Auftraggebers erfolgen über verschlüsselte Verbindungen.
- Daten, die im Rahmen der Datensicherung auf Band oder Festplatte gespeichert werden, werden verschlüsselt an das Datensicherungssystem übertragen und verschlüsselt gespeichert
- Alle zugangsberechtigten Administratoren des Auftragnehmers sind auf die Einhaltung der Sicherheitsrichtlinien des Auftragnehmers und auf das Datengeheimnis verpflichtet.

5. Eingabekontrolle

Zielbeschreibung: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.

- Die Verwaltung, Verarbeitung und Pflege von personenbezogenen Daten mittels Datenverarbeitungsprogrammen des Auftraggebers sowie die Protokollierung von Änderungen (Hinzufügen, Löschen, Ändern) an personenbezogenen Daten liegt im Verantwortungsbereich des Auftraggebers.

- Administrative Systemzugriffe werden adäquat protokolliert.
- Alle eingabeberechtigten Administratoren des Auftragnehmers sind auf die Einhaltung der Sicherheitsrichtlinien des Auftragnehmers und auf das Datengeheimnis verpflichtet.

6. Auftragskontrolle

Zielbeschreibung: Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

- Aufträge bzw. Weisungen des Auftraggebers werden schriftlich über ein CRM/Ticketsystem des Auftragnehmers erteilt oder bei Vorliegen eines schriftlichen Angebots durch den Auftraggeber schriftlich beauftragt und die Annahme durch den Auftragnehmer entsprechend bestätigt.
- Alle auftragsberechtigten Personen sind beim Auftragnehmer namentlich und mit E-Mail-Adresse bekannt
- Telefonisch erteilte Aufträge bzw. Weisungen werden durch den Auftragnehmer nur von persönlich bekannten Personen angenommen
- Alle Aufträge bzw. Weisungen und Arbeiten werden im CRM/Ticketsystem des Auftragnehmers dokumentiert.
- Der Auftragnehmer hat einen Datenschutzbeauftragten formal bestellt.

7. Verfügbarkeitskontrolle

Zielbeschreibung: Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Der Auftragnehmer betreibt eine Backup-Policy für eine regelmäßige Datensicherung.
- Die Datensicherungen des Auftragnehmers werden datenschutzkonform außerhalb des Rechenzentrums verwahrt.
- Eine Firewall schützt die Datenverarbeitungssysteme des Auftraggebers vor unberechtigten Zugriffen aus dem Internet.
- Die Rechenzentren verfügen über ausreichend dimensionierte Systeme für eine unterbrechungsfreie Stromversorgung (USV), Notstromversorgung mit Diesel-Generatoren, redundante Klimatisierungssysteme, Branderkennung und Brandbekämpfung.

8. Trennungskontrolle

Zielbeschreibung: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Die Trennung der Daten hinsichtlich ihrer bestimmungsgemäßen Verarbeitung (Entwicklungs-, Test- und Produktivsysteme) erfolgt durch systembasierte virtuelle Maschinen.
- Der Auftraggeber hat sicherzustellen, dass personenbezogenen Daten aus Produktivumgebungen vor Einspielen in Test- oder Entwicklungsumgebungen anonymisiert oder pseudonymisiert werden.
- In den zur Verfügung gestellten Systemen liegt eine logische Mandantentrennung (softwareseitig) vor.

Anhang 2: Genehmigte Unterauftragsverarbeitung und Meldung einer weiteren Unterauftragsverarbeitung

Genehmigte Unterauftragsverarbeitung

Folgender Subunternehmer wird im Zuge des genannten Hauptvertrages beauftragt:

Unternehmen	Anschrift	Auszuführende Leistung
GOOGLE CLOUD EMEA LIMITED	GOOGLE CLOUD EMEA LIMITED 70 Sir John Rogerson's Quay Dublin 2 Ireland https://cloud.google.com/	Hosting-Provider: Bereitstellung der Server Infrastruktur (inkl. Backups) und sicherheitsrelevanter Dienste für den Auftragnehmer Rechenzentrum innerhalb von Deutschland lokalisiert
METAWAYS INFOSYSTEMS GMBH	METAWAYS INFOSYSTEMS GMBH Schloßstraße 49 22967 Tremsbüttel Deutschland https://www.metaways.de/	Zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration und Wartung von Server-Systemen und Applikationen des Auftragnehmers Rechenzentrum innerhalb der EU lokalisiert

Meldung einer weiteren Unterauftragsverarbeitung

Folgender Subunternehmer wird im Zuge des genannten Hauptvertrages beauftragt:

Unternehmen	Anschrift	Auszuführende Leistung

Der Auftraggeber bestätigt die Zustimmung der obigen Unterauftragsdatenverarbeitung:

....

Ort / Datum Unterschrift