

Anlage 1

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

1. Vertragsgegenstand und Dauer

- 1.1 Der AUFTRAGNEHMER erbringt für den AUFTRAGGEBER Dienstleistungen im Bereich der Amazon PPC Beratung und Betreuung gemäß dem jeweiligen Leistungsangebot und den Allgemeinen Geschäftsbedingungen des AUFTRAGNEHMERS („**Hauptvertrag**“). Dabei erhält der AUFTRAGNEHMER Zugriff auf personenbezogene Daten, die dieser ausschließlich im Auftrag und nach Weisung des AUFTRAGGEBERS verarbeitet, sofern der AUFTRAGNEHMER nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Dem AUFTRAGGEBER obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.
- 1.2 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Auftragsverarbeitungsvertrag („**Vereinbarung**“). Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor. Die Rechte der betroffenen Personen bleiben durch diese Vereinbarung sowie den Hauptvertrag unberührt. Bestimmungen, die die Rechte der Betroffenen einschränken, entfalten gegenüber diesen Personen keine Wirksamkeit.
- 1.3 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der AUFTRAGNEHMER und seine Beschäftigten oder durch den AUFTRAGNEHMER beauftragte Empfänger im Auftrag des AUFTRAGGEBERS personenbezogenen Daten verarbeiten, für die der Auftraggeber als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO gilt.
- 1.4 Personenbezogene Daten des AUFTRAGGEBERS werden vom AUFTRAGNEHMER nur für die Dauer des Hauptvertrages zwischen den Parteien verarbeitet.

2. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten sowie Kategorien der von der Verarbeitung betroffenen Personen und die Zwecke, für die die personenbezogenen Daten im Auftrag des AUFTRAGGEBERS verarbeitet werden, sind in **Anhang 1** aufgeführt. Im Übrigen ergeben sich Umfang und Zweck der Datenverarbeitung durch den AUFTRAGNEHMER aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung).

3. Weisungsrecht

- 3.1 Der AUFTRAGNEHMER darf personenbezogene Daten des AUFTRAGGEBERS nur im Rahmen des Hauptvertrags und gemäß den Weisungen des AUFTRAGGEBERS erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der AUFTRAGNEHMER durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem AUFTRAGGEBER diese rechtlichen Anforderungen vor der Verarbeitung mit.

- 3.2 Die Weisungen des AUFTRAGGEBERS werden anfänglich durch diese Vereinbarung festgelegt und können vom AUFTRAGGEBER danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der AUFTRAGGEBER ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Der AUFTRAGGEBER wird gegenüber dem AUFTRAGNEHMER jeweils weisungsberechtigte Personen in Textform benennen. Bei einem Wechsel oder einer längerfristigen Verhinderung soll unverzüglich ein Nachfolger bzw. Vertreter der weisungsberechtigten Person benannt werden.
- 3.3 Weisungen sind vom AUFTRAGGEBER zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Der AUFTRAGNEHMER ist berechtigt, alternative und zumutbare Maßnahmen vorzuschlagen, die den Zweck der Weisung gleichermaßen erfüllen.
- 3.4 Ist der AUFTRAGNEHMER der Ansicht, dass eine Weisung des AUFTRAGGEBERS gegen datenschutzrechtliche Bestimmungen verstößt, hat er den AUFTRAGGEBER unverzüglich darauf hinzuweisen. Der AUFTRAGNEHMER ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den AUFTRAGGEBER bestätigt oder geändert wird. Der AUFTRAGNEHMER darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4. Pflichten des AUFTRAGNEHMERS

- 4.1 Der AUFTRAGNEHMER ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Unterlagen und Daten sind gegen die Kenntnisaufnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
- 4.2 Der AUFTRAGNEHMER wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieser Vereinbarung betraut werden, entsprechend zur Vertraulichkeit verpflichten, es sei denn sie unterliegen bereits einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung, und über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der Verpflichtung sicherstellen.
- 4.3 Der AUFTRAGNEHMER wird den AUFTRAGGEBER angesichts der Art der Verarbeitung nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Betroffenenrechte unterstützen. Sollte sich ein Betroffener direkt an den AUFTRAGNEHMER wenden, um die Betroffenenrechte erkennbar hinsichtlich der im Auftrag des AUFTRAGGEBERS verarbeiteten personenbezogenen Daten des AUFTRAGGEBERS wahrzunehmen, wird der AUFTRAGNEHMER dieses Ersuchen unverzüglich an den AUFTRAGGEBER weiterleiten. Der AUFTRAGGEBER wird dem AUFTRAGNEHMER den insoweit entstehenden Aufwand vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.
- 4.4 Der AUFTRAGNEHMER wird den AUFTRAGGEBER unter Berücksichtigung der Art der Verarbeitung und der dem AUFTRAGNEHMER zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der

Einhaltung der in Art. 32-36 DSGVO genannten Pflichten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden. Der AUFTRAGGEBER wird den AUFTRAGNEHMER den insoweit entstehenden Aufwand vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.

- 4.5 Bei Störungen, Verdacht auf Datenschutzverletzungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des AUFTRAGGEBERS wird der AUFTRAGNEHMER den AUFTRAGGEBER in angemessener Frist informieren. Dasselbe gilt für Prüfungen des AUFTRAGNEHMERS durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:
- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
 - c) eine Beschreibung der vom AUFTRAGNEHMER ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der AUFTRAGNEHMER trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den AUFTRAGGEBER und ersucht diesen um weitere Weisungen. Der AUFTRAGNEHMER ist darüber hinaus verpflichtet, dem AUFTRAGGEBER jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung des Datenschutzes betroffen sind.

- 4.6 Kontaktdaten des zuständigen Datenschutzteams des AUFTRAGNEHMERS (Data Protection Office) sind in **Anhang 2** dieser Vereinbarung aufgeführt.
- 4.7 Leistungen des AUFTRAGNEHMERS können unter dem Vorbehalt der Rechte Dritter und eigener Rechte stehen, insbesondere der Rechte betroffener Personen, berechtigter Interessen an der Vertraulichkeit sowie der Wahrung von IP-Rechten. Der AUFTRAGNEHMER ist berechtigt, Leistungen zu verweigern oder einzuschränken, bis der AUFTRAGGEBER entgegenstehende Rechte beseitigt.

5. Technische und organisatorische Maßnahmen

- 5.1 Der AUFTRAGNEHMER wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des AUFTRAGGEBERS gemäß Art. 32 DSGVO getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der AUFTRAGNEHMER zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen.
- 5.2 Die vom AUFTRAGNEHMER getroffenen technischen und organisatorischen Maßnahmen sind im **Anhang 3** dieser Vereinbarung spezifiziert. Der

AUFTRAGNEHMER überprüft regelmäßig, ob die technischen und organisatorischen Maßnahmen den Datenschutzvorschriften entsprechen und das vereinbarte Sicherheitsniveau weiterhin gewährleisten.

- 5.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem AUFTRAGNEHMER vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der AUFTRAGGEBER kann jederzeit eine aktuelle Fassung der vom AUFTRAGNEHMER getroffenen technischen und organisatorischen Maßnahmen anfordern. Über wesentliche Änderungen der technischen und organisatorischen Maßnahmen hat der AUFTRAGNEHMER den AUFTRAGGEBER in Textform zu unterrichten.

6. Kontrollrechte des AUFTRAGGEBERS

- 6.1 Der AUFTRAGGEBER überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten durch den AUFTRAGNEHMER, insbesondere der technischen und organisatorischen Maßnahmen. Auf Verlangen des AUFTRAGGEBERS gestattet der AUFTRAGNEHMER ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Kontrollrechte entfallen, wenn der AUFTRAGNEHMER die Einhaltung der Datenschutzvorschriften durch alternative Nachweise sicherstellt. Dies kann beispielsweise durch genehmigte Verhaltensregeln, Zertifizierungen oder Bestätigungen unabhängiger Dritter erfolgen. Vor der Durchführung eines Audits ist dem AUFTRAGNEHMER die Gelegenheit zu geben, solche Nachweise vorzulegen.
- 6.2 Der AUFTRAGGEBER kann die Prüfung selbst durchführen oder fachlich und persönlich geeignete, unabhängige Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des AUFTRAGNEHMERS umfassen und werden in der Regel mit angemessener Vorankündigung (mindestens 14 Tage im Voraus) durchgeführt, wenn dadurch der Zweck der Überprüfung nicht gefährdet würde. Der AUFTRAGGEBER wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des AUFTRAGNEHMERS dabei nicht unverhältnismäßig stören.
- 6.3 Kontrollen können von der Verpflichtung abhängig gemacht werden, dass die prüfenden Personen sich zu einer strengen vertraglichen Geheimhaltung verpflichten, insbesondere in Bezug auf Informationen, die keine personenbezogenen Daten des AUFTRAGGEBERS betreffen. Der AUFTRAGNEHMER ist berechtigt, einen Prüfer abzulehnen, wenn berechnete Interessen betroffen sind. Dazu zählen unter anderem die Rechte Dritter, bestehende Geheimhaltungsverpflichtungen, die Vertraulichkeit oder Sicherheit der IT-Ressourcen oder der Schutz sensibler Informationen, insbesondere gegenüber Wettbewerbern.
- 6.4 Der AUFTRAGGEBER trägt jegliche Kosten für Kontrollen, es sei denn, eine solche Kontrolle deckt eine wesentliche Verletzung der Vereinbarung durch den AUFTRAGNEHMER auf; in diesen Fällen trägt der AUFTRAGNEHMER die eigenen Kosten der Kontrolle. Falls sich aus einer Kontrolle ergibt, dass der AUFTRAGNEHMER seinen Verpflichtungen aus der Vereinbarung nicht nachgekommen ist, heilt der AUFTRAGNEHMER diese Verletzung in angemessener Frist auf eigene Kosten.

7. Einsatz von Unterauftragsverarbeitern

- 7.1 Der AUFTRAGNEHMER besitzt die allgemeine Genehmigung des AUFTRAGGEBERS für die Beauftragung von Unterauftragsverarbeitern. Eine Liste der zum Zeitpunkt des Vertragsschlusses genehmigten Unterauftragsverarbeiter ist in **Anhang 4** dieser Vereinbarung enthalten. Die Beauftragung weiterer Unterauftragsverarbeiter kann darüber hinaus nach der gesonderten Zustimmung des AUFTRAGGEBERS erfolgen.
- 7.2 Der AUFTRAGNEHMER unterrichtet den AUFTRAGGEBER rechtzeitig in Textform über geplante Änderungen bei der Beauftragung oder dem Austausch von Unterauftragsverarbeitern. Der AUFTRAGGEBER hat ausreichend Zeit ein, um vor der Beauftragung des betreffenden Unterauftragsverarbeiters bei berechtigten und nicht unerheblichen Beeinträchtigungen seiner Interessen schriftlich Einwände gegen diese Änderungen zu erheben. Einwände müssen konkret begründet werden. Sollte kein sachlich gerechtfertigter Grund für den Einwand vorliegen, kann der AUFTRAGNEHMER die Bereitstellung seiner Dienstleistungen einschränken oder den Hauptvertrag außerordentlich kündigen, insbesondere bei Unwirtschaftlichkeit der Leistungen ohne die geplanten Änderungen. Sofern der AUFTRAGNEHMER die Einwände des AUFTRAGGEBERS ausräumt, gilt die Änderung als genehmigt.
- 7.3 Beauftragt der AUFTRAGNEHMER einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des AUFTRAGGEBERS, so muss diese Beauftragung im Wege eines Unterauftragsverarbeitungsvertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den AUFTRAGNEHMER gemäß dieser Vereinbarung gelten. Der AUFTRAGNEHMER stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der AUFTRAGNEHMER entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.
- 7.4 Der AUFTRAGNEHMER koordiniert sämtliche Anfragen des AUFTRAGGEBERS in Bezug auf Unterauftragsverarbeiter und übermittelt Rückmeldungen oder Berichte entsprechend. Eine direkte Kontaktaufnahme des AUFTRAGGEBERS mit Unterauftragsverarbeitern ist nur in Ausnahmefällen gestattet, wenn eine Kommunikation über den AUFTRAGNEHMER nicht ausreicht, um gesetzlichen Anforderungen nachzukommen.
- 7.5 Eine Unterauftragsverarbeitung im Sinne dieser Bestimmungen liegt nicht vor, wenn der AUFTRAGNEHMER Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der AUFTRAGNEHMER für den AUFTRAGGEBER erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den AUFTRAGGEBER genutzt werden.

8. Internationale Datenübermittlung

- 8.1 Der AUFTRAGNEHMER übermittelt personenbezogene Daten in ein Land außerhalb des Europäischen Wirtschaftsraums („**Drittland**“) ausschließlich in den in den Anhängen festgelegten Fällen, aufgrund einer konkreten Vereinbarung mit dem AUFTRAGGEBER oder auf dessen dokumentierte Weisung.

8.2 Bei Datenübermittlungen in Drittländer gewährleistet der AUFTRAGNEHMER die Einhaltung aller Anforderungen aus Kapitel V DSGVO. Dies gilt gleichermaßen für Übermittlungen zwischen Drittländern, die unter der Kontrolle des AUFTRAGNEHMERS stehen.

8.3 Sollten sich die rechtlichen Grundlagen für Datentransfers in ein Drittland ändern, beispielsweise durch eine Entscheidung der Europäischen Kommission gemäß Artikel 45 Abs. 5 DSGVO, streben die Parteien an, einen alternativen Mechanismus nach Kapitel V DSGVO zu nutzen. Hierzu können insbesondere Standardvertragsklauseln gemäß Artikel 46 Abs. 2 DSGVO vereinbart werden. Der AUFTRAGGEBER darf seine Zustimmung zu einer solchen Anpassung nicht unbillig verweigern. Ziffer 7.2 findet entsprechend Anwendung.

9. Löschung von personenbezogenen Daten des AUFTRAGGEBERS

9.1 Während der Laufzeit und gemäß den Regelungen des Hauptvertrages kann der AUFTRAGGEBER jederzeit auf die personenbezogenen Daten des AUFTRAGGEBERS zugreifen.

9.2 Der AUFTRAGNEHMER wird alle ihm überlassenen personenbezogenen Daten des AUFTRAGGEBERS, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht, zum Ende der Laufzeit dieser Vereinbarung löschen. Dies betrifft auch etwaige Datensicherungen beim AUFTRAGNEHMER.

10. Haftung

10.1 Der AUFTRAGNEHMER haftet ausschließlich im Rahmen von Artikel 82 Abs. 2 Satz 2 DSGVO. Auf diese Haftung finden auch die weiteren Regelungen des Artikel 82 DSGVO Anwendung.

10.2 Soweit der AUFTRAGNEHMER nicht haftet, stellt der AUFTRAGGEBER den AUFTRAGNEHMER auf erstes Anfordern von Ansprüchen frei, die von betroffenen Personen oder Dritten im Zusammenhang mit dieser Vereinbarung geltend gemacht werden.

10.3 Die Haftung des AUFTRAGNEHMERS im Innenverhältnis ist auf die vom AUFTRAGGEBER im Kalenderjahr des Schadenseintritts zu zahlende Vergütung gemäß Hauptvertrag begrenzt, maximal jedoch auf eine Million Euro. Ist im Kalenderjahr keine Vergütung zu zahlen, beträgt die Haftungshöchstsumme 10.000,00 Euro.

10.4 Haftungsausschlüsse oder -beschränkungen finden keine Anwendung bei Vorsatz oder grober Fahrlässigkeit sowie bei Schäden an Leben, Körper oder Gesundheit.

10.5 Im Übrigen richtet sich die Haftung nach den Bestimmungen des Hauptvertrags.

11. Schlussbestimmungen

11.1 Die Parteien verpflichten sich, Änderungen oder Ergänzungen dieser Vereinbarung einvernehmlich zu vereinbaren, sofern dies erforderlich ist, um eine datenschutzkonforme Verarbeitung gemäß den geltenden Datenschutzvorschriften sicherzustellen.

- 11.2 Soweit diese Vereinbarung keine abschließenden Regelungen trifft, gelten die Bestimmungen des Hauptvertrags entsprechend.
- 11.3 Die Schlussbestimmungen der Allgemeine Geschäftsbedingungen des AUFTRAGNEHMERS zu anwendbarem Recht und Gerichtsstand finden Anwendung.

Anhang 1

Umfang der Verarbeitung; Datenkategorien; Betroffene Personen

- I. **Umfang der Verarbeitung:** Der Umfang der Verarbeitung richtet sich nach den Bestimmungen des Hauptvertrags.
- II. **Regelmäßig verarbeitete Datentypen:** Kontaktdaten; Berufsdaten; Kommunikationsdaten
- III. **Kategorien betroffener Personen:** Organmitglieder, Mitarbeiter oder Erfüllungsgehilfen des AUFTRAGGEBERS oder der mit ihm verbundenen Unternehmen i.S.v. §§ 15 ff. AktG; Geschäftspartner oder Mitarbeiter von Geschäftspartnern des AUFTRAGGEBERS
- IV. **Ort der Verarbeitung:** Europäische Union (EU) / Europäischer Wirtschaftsraum (EWR)

Anhang 2

Kontaktpersonen

- I. **AUFTRAGNEHMER:** eFly Data Protection Office, Neckarstraße 189-191, 70190 Stuttgart; E-Mail: datenschutz@efly-amz.com
- II. **AUFTRAGGEBER:** Der AUFTRAGGEBER informiert den AUFTRAGNEHMER über die entsprechenden Kontaktpersonen und -daten gemäß Ziffer 3.2 dieser Vereinbarung.

Anhang 3

Technische und organisatorische Maßnahmen (TOM)

Maßnahme	Zweck	Beschreibung
Zutrittskontrolle	Sicherstellung, dass nur autorisierte Personen Zugang zu Räumlichkeiten und Einrichtungen mit Datenverarbeitung erhalten	<ul style="list-style-type: none"> • Einsatz von Zutrittskontrollsystemen • Mechanische Türsicherungen und Zugangssperren zu sensiblen Bereichen
Zugangs- und Zugriffskontrolle	Verhinderung des unbefugten Zugriffs auf IT-Systeme und Daten	<ul style="list-style-type: none"> • Personalisierte Benutzerkonten mit rollenbasierten Zugriffsbeschränkungen • Verwendung von starken, regelmäßig zu erneuernden Passwörtern • Einsatz von Firewalls, Virenschutzprogrammen und Multi-Faktor-Authentifizierung (MFA)

Eingabekontrolle	Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen von Daten	<ul style="list-style-type: none"> ● Protokollierung von Logins und Logouts in den Systemen ● Dokumentation und Überwachung von Wartungsarbeiten und Änderungen an Daten ● Schutz von Audit-Logs vor Manipulationen
Auftragskontrolle	Sicherstellung der Einhaltung vertraglicher Regelungen zur Datenverarbeitung	<ul style="list-style-type: none"> ● Schriftliche Festlegung von Weisungen des AUFTRAGGEBERS ● Regelmäßige Kontrollen zur Einhaltung der vertraglich vereinbarten Auftragsverarbeitung ● Verwendung von vertraglich festgelegten Datenschutzklauseln
Trennungskontrolle	Gewährleistung der getrennten Verarbeitung von Daten verschiedener Kunden	<ul style="list-style-type: none"> ● Logische Trennung der Kundendaten verschiedener Kunden ● Erstellung detaillierter Zugriffskonzepte mit individuellen Berechtigungen ● Nutzung von mandantenfähigen Systemen
Weitergabekontrolle	Schutz der Daten bei Übertragung oder Weitergabe an Dritte	<ul style="list-style-type: none"> ● Einsatz von sicheren Übertragungsprotokollen (z. B. TLS, SFTP) ● Fachgerechte Vernichtung und Entsorgung von Papierakten und Speichermedien
Verfügbarkeit und Belastbarkeit	Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme und Daten	<ul style="list-style-type: none"> ● Regelmäßige und automatisierte Datensicherungen ● Einsatz von redundanten Speichersystemen innerhalb der eingesetzten Cloud-Infrastruktur ● Entwicklung und Implementierung eines Notfallplans ● Nutzung von Firewall- und Virenschutzsystemen zur Sicherung der IT-Infrastruktur

Organisationskontrolle	Sicherstellung ordnungsgemäßen Organisation Datenverarbeitung	der der	<ul style="list-style-type: none"> • Schulung der Mitarbeiter in Datenschutz und IT-Sicherheit • Entwicklung und Umsetzung eines IT-Sicherheitskonzepts • Implementierung eines Datenschutzteams (Data Protection Office) und regelmäßige Überprüfung der Prozesse
Privacy by Default und Privacy by Design	Sicherstellung datenschutzfreundlicher Prozesse und Voreinstellungen		<ul style="list-style-type: none"> • Implementierung transparenter und benutzerfreundlicher Datenschutzeinstellungen • Voreinstellungen in Systemen und Anwendungen, die nur die erforderlichen Daten erheben • Integration von Datenschutzanforderungen bereits in der Entwicklung von Produkten und Prozessen
Wirksamkeitskontrolle	Sicherstellung, dass die technischen und organisatorischen Maßnahmen effektiv und angemessen bleiben		<ul style="list-style-type: none"> • Überprüfung und Bewertung der Wirksamkeit der implementierten Maßnahmen • Durchführung von internen und externen Audits, um mögliche Schwachstellen zu identifizieren • Anpassung der Maßnahmen an neue Risiken, gesetzliche Anforderungen oder technische Entwicklungen

Anhang 4 Unterauftragsverarbeiter

Nr.	Unterauftragsverarbeiter	Beschreibung der Verarbeitung	Ort der Verarbeitung
1	Alphabet Inc.	Kommunikations- und Kollaborationsdienste (Workspace)	EU/EWR
2	Microsoft Corporation	Speicher- und Kollaborationsdiensten (Onedrive)	EU/EWR
3	Digital Butlers GmbH	Kampagnensteuerung	EU/EWR
4	BidX GmbH	Kampagnensteuerung	EU/EWR

5	nandu.ai GmbH	Prozessautomatisierung	EU/EWR
---	---------------	------------------------	--------