Auftragsverarbeitungsvertrag (AVV) nach Art. 28 Abs. 3 DSGVO

Auftraggeber (Verantwortlicher)

Auftragnehmerin (Auftragsverarbeiterin)

DevLabor GmbH
Altperverstraße 1-5
29410 Hansestadt Salzwedel

1. Gegenstand und Dauer der Vereinbarung

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Hauptvertrag (bzw. unserem Angebot und Angebotsannahme) gemachten Angaben und ist abhängig vom Bestand dieses Hauptvertrages. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses beendet gleichzeitig diese Vereinbarung.
Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

Bei Datenschutzverstößen wird dem Auftragsgeber ein Sonderkündigungsrecht eingeräumt.

Die Auftragnehmerin verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Im Falle einer Insolvenz oder eines vergleichbaren rechtlichen Verfahrens des Auftragnehmers verpflichtet sich dieser, umgehend alle notwendigen Schritte einzuleiten, um die Sicherheit und

Vertraulichkeit der vom Auftraggeber übertragenen Daten zu gewährleisten. Dies umfasst die sofortige Information des Auftraggebers über den insolvenzrechtlichen Status und die Bereitstellung aller relevanten Informationen bezüglich der gespeicherten Daten. Der Auftragnehmer muss sicherstellen, dass die Daten entweder gemäß den Anweisungen des Auftraggebers übertragen oder, falls eine Übertragung nicht möglich ist, unter Einhaltung der geltenden Datenschutzbestimmungen sicher und dauerhaft gelöscht werden. Es ist dem Auftragnehmer untersagt, die Daten zu eigenen Zwecken zu nutzen oder sie an Dritte weiterzugeben, es sei denn, dies ist zur Erfüllung der Anweisungen des Auftraggebers oder zur Einhaltung gesetzlicher Vorschriften erforderlich.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Soweit es sich nicht aus dem Vertragsinhalt der unter Ziffer 1 beschriebenen Vertragsverhältnisse ergibt, werden der Auftragnehmerin durch den Auftraggeber der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in Anlage 1 beschrieben. Somit werden in Anlage 1.

a) Art, Umfang und Zweck der Datenverarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO),

b) Art der zu verarbeitenden personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO),

c) Kategorie der Personen, deren Daten verarbeitet werden (entsprechend der Definition von Art. 4 Nr. 1 DSGVO)

gemäß den Angaben des Auftraggebers vertraglich festgehalten.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist die Auftragnehmerin verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

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

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

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

Der Auftraggeber informiert die Auftragnehmerin unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger der Auftragnehmerin

Weisungsberechtigte Personen neben dem Auftraggeber aus dem Hauptvertrag sind:

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger bei der Auftragnehmerin sind:

Jeffrey Reichardt, Geschäftsführer
Benjamin Ullrich, Geschäftsführer

Für Weisung zu nutzende Kommunikationskanäle:

DevLabor GmbH, Altperverstraße 1-5, 29410 Hansestadt Salzwedel
office@devlabor.com

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten der Auftragnehmerin

Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern sie nicht zu einer

anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO).

Die Auftragnehmerin 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.

Die Auftragnehmerin sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Sie sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Die Auftragnehmerin hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat die Auftragnehmerin im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 Buchstabe e und f DSGVO). Sie hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle neben des Auftraggebers aus dem Hauptvertrag weiterzuleiten:

Die Auftragnehmerin wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung ihrer Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Die Auftragnehmerin hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen der Auftragnehmerin dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Die Auftragnehmerin erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 Buchstabe h DSGVO).

Die Auftragnehmerin sichert zu, dass sie, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten der Auftragnehmerin) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

Die Auftragnehmerin bestätigt, dass ihr die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Sie verpflichtet sich, auch folgende für diesen Auftrag relevante Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

Die Auftragnehmerin verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 Buchstabe b und Art. 29 DSGVO). Die Auftragnehmerin überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb.

Bei der Auftragnehmerin ist als Beauftragte(r) für den Datenschutz Herr/Frau

Lars Paternoster (externer Datenschutzbeauftragter)
datenschutz@devlabor.com

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Sofern einschlägig: Die Auftragnehmerin verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

6. Mitteilungspflichten der Auftragnehmerin bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Die Auftragnehmerin teilt dem Auftraggeber unverzüglich Störungen, Verstöße der Auftragnehmerin oder der bei ihr beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Die Auftragnehmerin sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 Buchstabe f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf die Auftragnehmerin nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 Buchstabe d DSGVO)

Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, sind im Sinne dieser Regelung als Unterauftragsverhältnisse zu verstehen.
Von der Auftragnehmerin in Anspruch genommene Dienstleistungen, die lediglich zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen (z.B. Telekommunikations-/ Post-/ Transportdienstleistungen, Wartung, Benutzerservice) dienen, werden als Nebenleistung und im Sinne dieser Regelung nicht als Unterauftragsverhältnis betrachtet.
Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist der Auftragnehmerin nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn die Auftragnehmerin dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss die Auftragnehmerin dafür Sorge tragen, dass sie den Subunternehmer, sowie Nebendienstleister unter besonderer Berücksichtigung der Eignung der von diesem getroffenen

technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Die Auftragnehmerin hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmerin auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten der Auftragnehmerin und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Die Auftragnehmerin hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen: Jährliche Kontrolle und Überprüfung geeigneter Zertifikate durch den Datenschutzbeauftragten.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Die Auftragnehmerin haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch die Auftragnehmerin im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Über die bestehenden Unterbeauftragungsverhältnisse informiert der Auftragsverarbeiter über die folgende Webseite devlabor.com/subunternehmer. Falls nicht nachfolgend anders oder im Rahmen des Hauptvertrages definiert:

Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Bei einer Änderung der Subunternehmer informiert der Auftragsverarbeiter den Auftraggeber per E-Mail. Der Auftragsverarbeiter gewährleistet, dass bei einer Änderung der Unterbeauftragungsverhältnisse das Datenschutzniveau mindestens gehalten, wenn nicht sogar verbessert wird. Der Auftraggeber kann der Änderung innerhalb einer Frist von zwei Wochen aus wichtigem Grund gegenüber dem Auftragsverarbeiter widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als erteilt.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 Buchstabe c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt: Siehe Anlage 2 unter 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO).

Das im Anhang beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse bei der Auftragnehmerin dar.

Das im Anhang beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis bestehen:

Jährliche Kontrolle der Einhaltung beim Auftragnehmer und/oder Überprüfung Zertifikat(e) durch den Datenschutzbeauftragten samt Protokollierung.
Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmerin und Auftraggeber abzustimmen.

Soweit die bei der Auftragnehmerin getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt sie den Auftraggeber unverzüglich.

Die Maßnahmen bei der Auftragnehmerin können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss die Auftragnehmerin mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen der Auftragnehmerin nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 Buchstabe g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat die Auftragnehmerin sämtliche in ihrem Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

Auf ihren eigenen Datenträgern hat die Auftragnehmerin sämtliche Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

- Einsatz von Aktenvernichter der Sicherheitsstufe 4 (Partikelschnitt mit max. 2 mm Breite auf max. 15 mm Partikellänge; 30 mm Partikelfläche)
- Sicheres Löschen von Festplatten und Datenträgern

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Eine Vergütung für den Auftragsverarbeitungsvertrag wird nicht gefordert.
Soweit der Auftraggeber Unterstützung nach Ziffer 5 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.
Soweit der Auftraggeber Kontrollrechte ausüben wird, die nicht anlassbezogen sind, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung von der Auftragnehmerin abgestellten Mitarbeiters. Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 3, so hat er durch diese Weisung entstehende Kosten zu erstatten.

Sollten dabei zusätzliche Aufwände für den Auftragnehmer entstehen, erfolgt die Abrechnung zum Stundensatz von 110,- EUR zzgl. Umsatzsteuer, sofern im Hauptvertrag nicht anders geregelt.

11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Es werden folgende Zusatzvereinbarungen getroffen:

Datum:

_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmerin

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO:

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung, soweit es sich nicht aus dem Vertragsinhalt der unter Ziffer 1 beschriebenen Vertragsverhältnisse (Hauptvertrag) ergibt. Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten:

Umfang/Art der Daten & Zweck ihrer Verarbeitung

- Personenstammdaten *(Name, Vorname, Organisationseinheit, Anschrift)*
- Kommunikationsdaten *(Telefon, Mobilnummer, E-Mail)*
- Vertragsdaten
- Zugangsdaten im Rahmen des Vertrages
- Protokolldaten / IT-Nutzungsdaten

Kreis der betroffenen Personen

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

Anlage 2:

Technische und organisatorische Maßnahmen (TOMs) i.S.d. Art. 32 DSGVO (Stand 06.12.2024)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Manuelles Schließsystem	☑ Schlüsselregelung / Liste
☑ Sicherheitsschlösser	☑ Besucher in Begleitung durch Mitarbeiter
☑ Absicherung der Gebäudeschächte	☑ Sorgfalt bei Auswahl Reinigungsdienste
☑ Türen mit Knauf Außenseite	☑ Vier Augen Prinzip bei kritischen Prozessen
	☑ Zugang nur für berechtigte Mitarbeiter

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz

von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Login mit Benutzername + Passwort	☑ Verwalten von Benutzerberechtigungen
☑ Login mit biometrischen Daten	☑ Erstellen von Benutzerprofilen
☑ Einsatz VPN bei Remote-Zugriffen, wenn erforderlich	☑ Zentrale Passwortvergabe
☑ Anti-Virus-Software Clients	☑ Richtlinie „Sicheres Passwort“
☑ Verschlüsselung von externen Datenträgern	☑ Richtlinie „Löschen / Vernichten“
☑ Firewall	☑ Richtlinie „Clean desk“
☑ Automatische Desktopsperre	☑ Allg. Richtlinie Datenschutz und / oder Sicherheit
☑ Verschlüsselung von Notebooks / Tablet	☑ Richtlinie „Mobiles Arbeiten”
	☑ Anleitung „Manuelle Desktopsperre“

1.3 Zugriffskontrolle

Maßnahmen, die 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 Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**

☑ Aktenschredder (mind. Stufe 4)	☑ Einsatz Berechtigungskonzepte
☑ Verwaltung Benutzerrechte durch Administratoren	☑ Minimale Anzahl an Administratoren
☑ Physische Löschung von externen Datenträgern	

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Trennung von Produktiv- und Testumgebung	☑ Steuerung über Berechtigungskonzept
☑ Mandantenfähigkeit relevanter Anwendungen	☑ Festlegung von Datenbankrechten

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	**Organisatorische Maßnahmen**
	☑ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ E-Mail Verbindungsverschlüsselung (SSL/TLS)	☑ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☑ Einsatz von VPN	☑ Anlassbezogene Sichtung von Abruf- und Übermittlungsvorgängen
☑ Protokollierung der VPN Zugriffe und Abrufe	
☑ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☑ Nutzung von Signaturverfahren (SSL generell und elektronische Signatur im Bedarfsfall)	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung)

stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten gemäß Hauptvertrag und Weisung des Auftraggebers	☑ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☑ Manuelle oder automatisierte Kontrolle der Protokolle gemäß Hauptvertrag und Weisung des Auftraggebers	☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☑ Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.
Wir verweisen auf die entsprechenden technischen und organisatorischen Maßnahmen der Subunternehmer unter devlabor.com/subunternehmer.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen

☑ Software-Lösungen für Datenschutz-Management im Einsatz	☑ Externer Datenschutzbeauftragter Lars Paternoster (extern) datenschutz@devlabor.com
☑ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	☑ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☑ Anderweitiges dokumentiertes Sicherheitskonzept	☑ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
☑ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durch den externen Datenschutzbeauftragten durchgeführt	☑ Interner Informationssicherheitsbeauftragter (in Vorbereitung) Benjamin Ullrich (DevLabor GmbH) ullrich@devlabor.com
	☑ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☑ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von Firewall und regelmäßige Aktualisierung	☑ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☑ Einsatz von Spamfilter und regelmäßige Aktualisierung	☑ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☑ Einsatz von Virenscanner und regelmäßige Aktualisierung	☑ Einbindung von ☑ DSB und ☑ ISB in Sicherheitsvorfälle und Datenpannen
	☑ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	☑ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☑ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
	☑ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☑ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	☑ Schriftliche Weisungen an den Auftragnehmer
	☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☑ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☑ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☑ Regelung zum Einsatz weiterer Subunternehmer (siehe devlabor.com/subunternehmer)

	☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☑ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus