

# Auftragsdatenverarbeitungsvertrag

Zwischen dem/der

.....  
- Verantwortlicher - nachstehend Auftraggeber genannt -

.....  
- Firmenanschrift -

und der

SüdniedersachsenStiftung  
Welcome Centre  
Maschmühlenweg 105  
37081 Göttingen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

## 1. Gegenstand und Dauer des Vertrags

### (1) Gegenstand

Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: siehe Anlage 3 (Beschreibung der Aufgaben).

(2) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

### (3) Dauer

Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 3 Monaten zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(4) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

## **2. Konkretisierung des Vertragsinhalts**

### **(1) Art und Zweck der vorgesehenen Verarbeitung von Daten**

Das Welcome Centre, als eine Abteilung der SüdniedersachsenStiftung, verarbeitet personenbezogene Daten zum Zwecke der Beratung und Unterstützung von zuwandernden und zugewanderten (potenziellen) Fachkräften sowie gegebenenfalls deren Familienangehörigen. Ziele sind beispielsweise die Beantragung von Visa, Meldung bei Behörden, Beantragung von Kindergeld, Vermittlung von Mietwohnungen, Vermittlung von Schul- sowie Kinderbetreuungsplätzen sowie sämtliche weiteren Dienstleistungsangebote des Welcome Centres. Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung (Anlage 3).

### **(2) Art der Daten**

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) je nach beauftragter Leistung:

Name, Vorname, Geburtsdatum, Geburtsort, Nationalität, Anschrift, Titel, Anrede, E-Mail-Adresse, Telefonnummer, Familienstand, Arbeitsvertrag, Stellenbeschreibung, Gehaltsabrechnungen, Steuer ID, Ausweisdokumente, Arbeits-/Aufenthaltsgenehmigungen, Bankdaten, gesundheitliche Informationen (z.B. Impfpass, Krankenkassenkarte), Führerschein, Renten- und Sozialversicherungsnummer, Personenstandsurkunden, Zeugnisse und Vollmachten sowie sämtliche Angaben die notwendig sind, um die gewünschten Dienstleistungen zu erfüllen, wie etwa behördliche Anträge zu stellen, Visa oder eAT zu beantragen, zu prüfen oder abzuholen, Einschulungen vorzunehmen, Mietverträge abzuschließen (Schufa-Auskunft, Mieterselbstauskunft) etc. Ggfs. werden die gleichen Daten von Angehörigen benötigt.

### **(3) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte (inklusive Bewerbende) des Auftraggebers
- Angehörige von Beschäftigten (inklusive Bewerbende) des Auftraggebers.

## **3. Technisch-organisatorische Maßnahmen**

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags. Soweit die Prüfung /ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber in Kenntnis zu setzen.

(3) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 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 [Einzelheiten in Anlage 1].

#### **4. Rechte von betroffenen Personen**

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, 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.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

#### **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Die Wahrung der Vertraulichkeit gemäß Artt. 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 berechtigterweise 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.

- b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- e) Der Auftragnehmer kontrolliert regelmäßig die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1], 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.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.
- g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

## **6. Unterauftragsverhältnisse**

(1) 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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in Anlage 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Anlage 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht überschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers, sofern dies nicht vorab genehmigt wurde. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **7. Internationale Datentransfers**

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

Die Beauftragung weiterer Dienstleister in Drittstaaten folgt dem Ablauf nach 6. dieses Vertrages.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

## **8. Kontrollrechte des Auftraggebers**

(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 rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen. Die Kosten dieser Überprüfung des Auftragnehmers trägt der Auftraggeber. Diese Kosten werden dem Auftraggeber vorab mitgeteilt und richten sich nach dem Zeitaufwand für das einzusetzende begleitende Personal sowie die Erläuterungen.

(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.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## **9. Weisungsbefugnis des Auftraggebers**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## **10. Löschung und Rückgabe von personenbezogenen Daten**

(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.

(2) Nach Abschluss der nach der Leistungsvereinbarung vereinbarten (Einzel-)Leistungen oder früher nach Aufforderung durch den Auftraggeber 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

.....  
Ort, Datum

.....  
Auftraggeber

.....  
Ort, Datum

.....  
Auftragnehmer

## **Anlage 1 - Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO**

### **Grundsätzliche Maßnahmen**

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virens Scanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Das Reinigungspersonal sowie übrige Dienstleister:innen, die zur Erfüllung nebensächlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

- Die an Mitarbeitende ausgegebene Schlüssel sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung überwacht und anlassbezogen evaluiert wird.

## **Zutrittskontrolle**

- Während der Hauptgeschäftszeiten ist sichergestellt, dass das Büro mit Personal besetzt ist.
- Die Eingangstür zu den Stiftungsräumen ist stets verschlossen. Besucher:innen werden nur durch Beschäftigte eingelassen. Mitarbeitende sind angewiesen Besucher:innen stets zu begleiten.
- Den Welcome Centre Mitarbeitenden wird ein eigener Büroraum zur Verfügung gestellt, der nicht von anderen Mitarbeitenden genutzt werden darf.
- Sollten es von Nöten sein, (Kopien von) Dokumente(n) mit sensiblen Daten für die Bearbeitung des Falls zu erstellen oder aufzubewahren, wird sichergestellt, dass diese in abschließbaren Schränken aufbewahrt werden.

## **Zugangskontrolle / Zugriffskontrolle**

- Im Bereich IT-Sicherheit wird auf stets aktuelle Softwareversionen und Virenschutz geachtet. Zudem werden die Daten des Welcome Centres durch eine Firewall (Soft- und Hardware) geschützt.
- Es erfolgt eine Authentifikation mit Benutzer und Passwort. Darüber hinaus wird auch eine Multifaktor-Authentifizierung ausgeführt.
- Es existiert eine Verschlüsselung von mobilen Datenträgern und Geräten sowie eine Verschlüsselung der Festplatte durch Bitlocker.
- Eine Protokollierung von Zugriffen auf Daten erfolgt.
- Es wird eine ordnungsgemäße Entsorgung von Datenträgern vorgenommen.
- Es wird dafür Sorge getragen, dass mittels Berechtigungs-/ Authentifizierungskonzepten der Zugriff auf sensible Daten auf den Personenkreis beschränkt bleibt, der mit den Daten arbeiten muss.

## **Weitergabekontrolle**

- Dokumente mit sensiblen Daten werden nur verschlüsselt an verschiedene Empfänger versandt. Auch die Übermittlung dieser Daten an das Welcome Centre durch Kund:innen oder Klient:innen erfolgt verschlüsselt.
- Für die Weitergabe von Dokumenten mit sensiblen Daten an Behörden wird ein elektronisches Behördenpostfach genutzt.

## **Eingabekontrolle**

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts, bei dem nur im Welcome Centre beschäftigte Mitarbeitende Zugriff auf Kunden- und Klientendaten erhalten.
- Die Protokollierung von Dateneingaben-, Änderungen und Löschungen erfolgt stets.

## **Auftragskontrolle**

- Es wird sichergestellt, dass Dokumente, die sensible Daten von Kund:innen und /oder Klient:innen enthalten nach Beendigung des Auftrages vernichtet werden.

## **Verfügbarkeitskontrolle / Integrität**

- Neben einem ständig kontrolliertem Backup- und Recoverykonzept wird zusätzlich dafür gesorgt, dass Sicherungskopien von allen Dokumenten auf einem lokalen Server gesichert werden. Dieser befindet sich an einem gesicherten Ort, zu dem nur ein beschränkter Personenkreis Zugriff hat.
- Es erfolgt der Einsatz von Festplattenspiegelungen.

## **Gewährleistung des Zweckbindungs-/Trennungsgebotes**

- Neben einer logischen Mandantentrennung (Software) erfolgt auch eine physische Mandantentrennung (Hardware).

## Anlage 2 - Genehmigte Unterauftragsverhältnisse

Firma Unterauftrag nehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland*
Microsoft Limited	One Microsoft Way Redmond, WA 98052-6399 USA	Bereitstellung M365 in europäischem Rechenzentrum	Es besteht eine Zertifizierung des Unternehmens nach dem „EU-US Data Privacy Framework“.: Mithin liegt ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DS-GVO vor.
Mailstore	Clörather Str. 1-3 41748 Viersen Deutschland	Archivierung von E-Mails	
procilon GmbH	Leipziger Straße 110 04425 Taucha bei Leipzig Deutschland	Bereitstellung elektronisches Behördenpostfach	
Starface GmbH	Adlerstraße 61 76137 Karlsruhe Deutschland	Bereitstellung Telefonie und Fax	

---

\* An dieser Stelle kommen insbesondere die Standarddatenschutzklauseln der Kommission gem. Art. 46 Abs. 2 lit. c DS-GVO in der Variante „Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter“ (Modul 3) in Betracht.