

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen der

BürgerStiftung Hamburg – Schopenstehl 31 – 20095 Hamburg

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

Firma – Str. Nr. – PLZ Ort

Kunden-Nr.:

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung des Hauptvertrages vom auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zum gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung in ein Drittland, welches ein durch Angemessenheitsbeschluss der Kommission festgestelltes angemessenes Schutzniveau aufweist (Art. 45 Abs. 3 DSGVO), bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, solange diese besonderen Voraussetzungen vorliegen. Jede sonstige Verlagerung in ein Drittland ist ausgeschlossen.

Bitte beachten Sie hierzu dringend das EuGH-Urteil vom 16.07.2020 (Az: C-311/18), welches das EU-US-Privacy Shield für ungültig erklärt und an die Pflichten für Datenexporteure und Datenimporteure bei Anwendung der EU-Standardvertragsklauseln, insbesondere hinsichtlich einer rechtskonformen Datenübermittlung, erinnert. [siehe auch Anlage 3]

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ...

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte

- Lieferanten
- Handelsvertreter
- Ansprechpartner
- ...

(4) Verarbeitungstätigkeiten [OPTIONAL]

Folgende Verarbeitungstätigkeiten sollen ausgeführt werden:

- Erheben
- Erfassen
- Organisieren
- Ordnen
- Speichern
- Anpassen
- Verändern
- Offenlegen durch Übermitteln/Verbreiten/andere Form der Bereitstellung
- Abgleich
- Verknüpfung
- Einschränkung
- Löschen/Vernichten
- ...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [**Anlage 1**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate

Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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 Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt:

Herr/Frau _____
Vorname, Name, Organisationseinheit, Telefon, E-Mail

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.

Als Ansprechpartner beim Auftragnehmer wird benannt:

Herr/Frau _____
Vorname, Name, Organisationseinheit, Telefon, E-Mail

oder

Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union:

Herr/Frau _____
Vorname, Name, Organisationseinheit, Telefon, E-Mail

- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die

Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Anlage 1].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- i) 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 der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

Herr/Frau _____

Vorname, Name, Organisationseinheit, Telefon, E-Mail

gewünschter Übertragungsweg

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

(1) Die Beauftragung von Unterauftragnehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche schriftlich oder in einem elektronischen Format erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Unterauftragnehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Das Schutzniveau, welches sich aus den zwischen Auftraggeber und Auftragnehmer für die konkrete Verarbeitung vereinbarten technischen und organisatorischen Maßnahmen **[Anlage 1]** ergibt, darf in keinem Fall unterschritten werden. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Auftragnehmer hat vertraglich sicherzustellen, dass alle vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(4) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit 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 DSGVO zugrunde gelegt wird.

[siehe auch Anlage 3]

(5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden. Der Auftragnehmer haftet für das Verschulden seines Subunternehmers wie für eigenes Verschulden.

(7) 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.

(8) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(9) Zurzeit sind für den Auftragnehmer die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

7. Kontrollrechte des Auftraggebers

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

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen [**Anlage 1**] nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

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

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

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

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Weisungsbefugnis des Auftraggebers

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

(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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Weisungsberechtigte Personen auf Seiten des Auftraggebers **[bitte mind. 2 Personen benennen]**:

Weisungsempfänger auf Seiten des Auftragnehmers **[bitte mind. 2 Personen benennen]**:

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 vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung

dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

(1) Auf Art. 82 DSGVO wird verwiesen.

12. Schlussbestimmung

(1) Folgende Anlagen sind fester Bestandteil dieses Vertrags:

Anlage 1 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Anlage 2 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Anlage 3 Ort der Verarbeitung

Anlage 4 Änderungsmitteilung für Auftragnehmer (im Bedarfsfall zu verwenden)

Die Anlagen können angepasst werden; die jeweils neue Version wird dabei automatisch Vereinbarungsbestandteil. Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für einen Verzicht auf dieses Schriftformerfordernis. Mündliche Nebenabreden bestehen nicht.

- (2) 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.
- (3) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
- (4) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.
- (5) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (6) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. An die Stelle der unwirksamen Bestimmung tritt eine Ersatzregelung, die dem mit der unwirksamen Bestimmung angestrebten Zweck möglichst nahekommt. Entsprechendes gilt für Vereinbarungslücken.

Ort, Datum

.....
Ort, Datum

Stempel u. Unterschrift
Auftraggeber

.....
Stempel u. Unterschrift
Auftragnehmer

Anlage 1

Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Hinweis:

1. Alternativ zur Beantwortung der nachfolgenden Checkliste kann ein eigenes Verzeichnis der Technisch-Organisatorischen Maßnahmen angegeben werden.
2. Ein Zertifikat für Verantwortliche mit geprüftem ISMS für das Management der Informationssicherheit (z. B. ISO 27 001) ggf. auf Basis BSI Grundschrift, kann die Beantwortung der nachfolgenden Fragen teilweise ersetzen.

Bitte fügen Sie in diesem Fall einen Nachweis für das Zertifikat bei und weisen in der Checkliste darauf hin.

3. Bei der Beantwortung der Fragen wählen Sie in der Spalte „**Umsetzung**“ aus den Werten:
 - **Ja**, entsprechend des aktuellen Umsetzungsstandes.
 - **Ja (gem. Zertifikat)**, entsprechend des aktuellen Umsetzungsstandes.
 - **Nein**, entsprechend des aktuellen Umsetzungsstandes.
 - **N/A**, wenn diese Maßnahme in Ihrem Fall nicht auf Sie zutreffend ist.

oder

 - Binden Sie ein **Umsetzungsdatum** ein, wenn die Maßnahme aktuell bei Ihnen umgesetzt wird.
4. Weitere Maßnahmenbeschreibungen können hinzugefügt werden. Diese können Sie auch als eigenes Dokument anfügen und müssen sich nicht an die Tabellenform halten.

Technische und organisatorische Maßnahmen Checkliste	Umsetzung
Auftragskontrolle (Unterauftragnehmer) <i>Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers (z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen)</i>	
organisatorisch	
Auftragsdatenverarbeitungsvertrag	<input type="checkbox"/>
Laufende Überprüfung des Auftragnehmers	<input type="checkbox"/>
Prüfung der TOM des Auftragnehmers	<input type="checkbox"/>
Sichere Datenvernichtung nach Auftragsende	<input type="checkbox"/>
Vereinbarung von Kontrollrechten	<input type="checkbox"/>
Vereinbarung von Vertragsstrafen	<input type="checkbox"/>
Verpflichtung auf Datengeheimnis gem BDSG-neu	<input type="checkbox"/>
Sorgfältige Auswahl des Auftragnehmers	<input type="checkbox"/>
Sorgfältige Vertragsgestaltung	<input type="checkbox"/>
Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber	<input type="checkbox"/>
Formalisierung der Auftragserteilung	<input type="checkbox"/>
Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung	<input type="checkbox"/>
Speicherung des Veranlassers für jeden Auftrag	<input type="checkbox"/>
Benutzerkontrolle	
organisatorisch	
Passwortrichtlinie (Regelung von Passwortregeln und Passwortwechsel)	<input type="checkbox"/>
Verwaltung von Benutzerberechtigungen	<input type="checkbox"/>
Verwaltung von Benutzerprofilen	<input type="checkbox"/>
Bedienungs- und Benutzeranweisungen	<input type="checkbox"/>
Einsatz von Programmierrichtlinien	<input type="checkbox"/>
Erlass von Datenschutzrichtlinien und Dienstanweisungen	<input type="checkbox"/>
Funktionstrennung innerhalb des IT-Bereichs	<input type="checkbox"/>
Regelungen zu Entwicklung, Test und Freigabe bei IT-Änderungen	<input type="checkbox"/>
Release- und Konfigurationsmanagement für IT-Systeme und Anwendungen	<input type="checkbox"/>
Schulung der Mitarbeiter	<input type="checkbox"/>
Vorgabe der Regelungen für die Passwortvergabe und -verwaltung	<input type="checkbox"/>
Vorgaben für die Dokumentation selbsterstellter Software	<input type="checkbox"/>
technisch	
Anti-Viren-Software	<input type="checkbox"/>
Authentifikation mit Benutzername und Passwort	<input type="checkbox"/>
Authentifikation mit biometrischen Merkmalen	<input type="checkbox"/>
Mobile Device Management (z. B. Blackberry Enterprise Server)	<input type="checkbox"/>
Sperren externer Schnittstellen (z. B. USB-Anschlüsse)	<input type="checkbox"/>
Verschlüsselung von Datenträgern	<input type="checkbox"/>
Verschlüsselung von Smartphones (z. B. Zwang durch BES-Policy)	<input type="checkbox"/>

Einsatz einer Firewall	<input type="checkbox"/>
Einsatz von VPN	<input type="checkbox"/>
Protokollierung der Benutzeraktivitäten	<input type="checkbox"/>
sichere Gehäuseverriegelung	<input type="checkbox"/>
Datenintegrität	
organisatorisch	
Bezug von Software nur von sicheren Quellen	<input type="checkbox"/>
technisch	
Sicherung der Software durch digitale Signaturen oder Hashwerte	<input type="checkbox"/>
Verschlüsselung der Datenträger	<input type="checkbox"/>
Verschlüsselung der internen Übertragungswege (z. B. SSL)	<input type="checkbox"/>
Verschlüsselung von Dateien und Datenbanken	<input type="checkbox"/>
Datenträgerkontrolle	
technisch	
Gehäuseverriegelung der Transportbehälter	<input type="checkbox"/>
Sperren externer Schnittstellen (z. B. USB-Anschlüsse)	<input type="checkbox"/>
Verschlüsselung von Datenträgern	<input type="checkbox"/>
Absicherung der Bereiche, in denen Datenträger aufbewahrt werden (Datenträgerarchiv)	<input type="checkbox"/>
Aufbewahrung von Datenträgern in Data Safes	<input type="checkbox"/>
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	<input type="checkbox"/>
Maschinelle Datenträgerverwaltung	<input type="checkbox"/>
Protokollierung der autorisierten Weitergabe und Entfernung von Datenträgern	<input type="checkbox"/>
Protokollierung der Kopie von Datenträgern	<input type="checkbox"/>
Eingabekontrolle	
<i>Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement</i>	
organisatorisch	
Archivierung von Eingabefeldern	<input type="checkbox"/>
Berechtigungsprofile für Eingabe, Änderung und Löschung	<input type="checkbox"/>
Dokumentation der Anwendung zur Datenverwaltung	<input type="checkbox"/>
Protokollierung der Benutzeraccounts für die Datenverwaltung	<input type="checkbox"/>
technisch	
Protokollierung von Eingabe, Änderung und Löschung	<input type="checkbox"/>

Speicherkontrolle	
organisatorisch	
Trennung des Test- und Produktionsbetriebes	<input type="checkbox"/>
technisch	
Verwaltung von Benutzerberechtigungen	<input type="checkbox"/>
Verwaltung von Benutzerprofilen	<input type="checkbox"/>
Datenverschlüsselung	<input type="checkbox"/>
Kontrolle und Trennung von System- und User-Aktivitäten	<input type="checkbox"/>
Revisionsfähigkeit der Zugriffsberechtigungsverwaltung	<input type="checkbox"/>
Softwareverriegelung des Bildschirms bei Inaktivität des Benutzers	<input type="checkbox"/>
Verwendung des Schreibschutzes bei Datenträgern	<input type="checkbox"/>
Transportkontrolle	
organisatorisch	
Dokumentation der Abruf- und Übermittlungsvorgänge	<input type="checkbox"/>
Dokumentation der Datenempfänger, Überlassungsfristen und Löschfristen	<input type="checkbox"/>
Sorgfältige Auswahl von Transportdienstleistern	<input type="checkbox"/>
Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	<input type="checkbox"/>
Festlegung des Berechtigten für die Übermittlung oder den Transport	<input type="checkbox"/>
Regelungen für die Versandart und Festlegung des Transportweges	<input type="checkbox"/>
Sicherung des Übertragungs- und Transportweges	<input type="checkbox"/>
Überwachung der Transportzeit	<input type="checkbox"/>
technisch	
Einrichtung von VPN-Tunneln	<input type="checkbox"/>
E-Mail-Verschlüsselung	<input type="checkbox"/>
Sichere Transportbehälter	<input type="checkbox"/>
Sicheres Löschen	<input type="checkbox"/>
Überprüfung von Datenträgern auf Virenbefall	<input type="checkbox"/>
Trennbarkeit	
<i>Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden (z.B. mandantenfähigkeit, Sandboxing)</i>	
organisatorisch	
Trennung von Datenbanken durch Berechtigungen	<input type="checkbox"/>
Berechtigungskonzept für Anwendungen, Laufwerke und Dateien	<input type="checkbox"/>
Organisatorische Berücksichtigung der Mandantentrennung	<input type="checkbox"/>
technisch	
getrennte Aufbewahrung der Zuordnungsdatei bei Pseudonymisierung	<input type="checkbox"/>
Physikalisch getrennte Systeme	<input type="checkbox"/>
Trennung durch getrennte Verschlüsselung	<input type="checkbox"/>
Trennung von Produktiv- und Testsystem	<input type="checkbox"/>
Verwendung von Software, die eine buchhalterische Mandantentrennung ermöglicht	<input type="checkbox"/>

Verfügbarkeitskontrolle	
<i>Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne</i>	
organisatorisch	
Notfallplan	<input type="checkbox"/>
Serverräume nicht unter wasserführenden Leitungen	<input type="checkbox"/>
Serverräume über der Grundwasserlinie	<input type="checkbox"/>
Test der Datenwiederherstellung	<input type="checkbox"/>
Backup- und Recovery-Konzept	<input type="checkbox"/>
Datenauslagerung an sicherem und ausgelagertem Ort	<input type="checkbox"/>
technisch	
Automatisierte Systemüberwachung und Alarmierung	<input type="checkbox"/>
Feuchtigkeitsüberwachung	<input type="checkbox"/>
Feuer- und Rauchmeldeanlagen	<input type="checkbox"/>
Feuerlöschgeräte in Serverräumen	<input type="checkbox"/>
Klimaanlage in Serverräumen	<input type="checkbox"/>
Schutzsteckdosen in Serverräumen	<input type="checkbox"/>
Temperaturüberwachung	<input type="checkbox"/>
USV - Unterbrechungsfreie Stromversorgung	<input type="checkbox"/>
regelmäßige und mehrstufige Datensicherung	<input type="checkbox"/>
Wiederherstellbarkeit	
<i>Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)</i>	
organisatorisch	
Notfallplan	<input type="checkbox"/>
Mehrstufiges Backup- und Restorekonzept	<input type="checkbox"/>
Sicherheits-Vorfall-Management	<input type="checkbox"/>
Notfallkonzept	<input type="checkbox"/>
technisch	
Backup- und Restoreautomatisierung	<input type="checkbox"/>
Zugangskontrolle	
<i>Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern</i>	
organisatorisch	
Ausweistragepflicht für Besucher	<input type="checkbox"/>
Ausweistragepflicht für Mitarbeiter	<input type="checkbox"/>
Personenkontrolle am Eingang	<input type="checkbox"/>
Protokollierung der Besucher (Besucherbuch)	<input type="checkbox"/>
Protokollierung der Schlüsselausgabe (Schlüsselbuch)	<input type="checkbox"/>
Sorgfältige Auswahl des Reinigungspersonals	<input type="checkbox"/>
Sorgfältige Auswahl des Sicherheitspersonals	<input type="checkbox"/>
Einrichtung von Schutz- und Sicherheitszonen	<input type="checkbox"/>

Festlegung der zugangsberechtigten Personen	<input type="checkbox"/>
Revisionsfähigkeit der Zugangsberechtigungen	<input type="checkbox"/>
technisch	
Absicherung von Gebäudeschächten	<input type="checkbox"/>
Alarmanlage	<input type="checkbox"/>
Automatisches Zugangskontrollsystem	<input type="checkbox"/>
Bewegungsmelder	<input type="checkbox"/>
Manuelles Schließsystem	<input type="checkbox"/>
Schließsystem mit Zugangscode	<input type="checkbox"/>
Sicherheitsschlösser	<input type="checkbox"/>
Videoüberwachung der Zugänge	<input type="checkbox"/>
Netzwerksegmentierung	<input type="checkbox"/>
NAC - Network Access Control	<input type="checkbox"/>
Automatische Bildschirmsperre	<input type="checkbox"/>
Protokollierung der Zu- und Abgänge	<input type="checkbox"/>
Zugriffskontrolle	
<i>Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen</i>	
organisatorisch	
minimierte Anzahl von Administratoren	<input type="checkbox"/>
Passwortrichtlinie (Regelung von Passwortregeln und Passwortwechsel)	<input type="checkbox"/>
Sichere Aufbewahrung von Datenträgern	<input type="checkbox"/>
Sichere Verwaltung von Benutzerrechten	<input type="checkbox"/>
zertifizierte Dienstleister für Akten- und Datenvernichtung	<input type="checkbox"/>
Regelmäßige Überprüfung der Berechtigungen	<input type="checkbox"/>
Revisionsfähiges Rollen-, Berechtigungs- und Nutzerkonzept	<input type="checkbox"/>
Regelungen zur Verlustmeldung und Reaktionen auf Datenträgerverlust	<input type="checkbox"/>
technisch	
Aktenvernichter	<input type="checkbox"/>
Datenträger-Vernichtung (DIN 32757)	<input type="checkbox"/>
Physische Löschung von Datenträgern vor Wiederverwendung	<input type="checkbox"/>
Protokollierung der Datenvernichtung	<input type="checkbox"/>
Protokollierung der Eingabe, Veränderung und Löschung von Daten	<input type="checkbox"/>
Verschlüsselung von Datenträgern	<input type="checkbox"/>
Verschlüsselung von Smartphones (z. B. Zwang durch BES-Policy)	<input type="checkbox"/>
Beschränkung der freien Abfragemöglichkeiten von Datenbanken (Query-Spache)	<input type="checkbox"/>
Zeitliche Begrenzung der Zugriffsmöglichkeiten	<input type="checkbox"/>

Zuverlässigkeit		
organisatorisch		
mindestens jährliche und dokumentierte Überprüfung der technischen und organisatorischen Maßnahmen		<input type="checkbox"/>
Regelung zur Reaktion auf Störungen		<input type="checkbox"/>
SLA für IT-Leistungen		<input type="checkbox"/>
Zentrale Beschaffung von Hard- und Software		<input type="checkbox"/>
technisch		
Virenschutz		<input type="checkbox"/>
Malwarescan		<input type="checkbox"/>
Penetrationstests		<input type="checkbox"/>
Regelmäßiges und zeitnahes Patch-Management		<input type="checkbox"/>
Übertragungskontrolle		
organisatorisch		
Festlegung der Übermittlungswege und der Datenempfänger		<input type="checkbox"/>
Org. Regelungen zur Einrichtung, Genehmigung und Befristung von Fernzugriffen (z.B. VPN)		<input type="checkbox"/>
Regelungen zum Einsatz mobiler Datenträger		<input type="checkbox"/>
Regelungen zum Einsatz von Cloud-Diensten		<input type="checkbox"/>
Regelungen zum E-Mail-Versand		<input type="checkbox"/>
technisch		
Automatisierte Überwachung nach außen offener Ports, Protokolle und Dienste		<input type="checkbox"/>
Protokollierung der Datenübermittlung inkl. Abrufer und Empfänger		<input type="checkbox"/>
Zeitbegrenzung von Zugriffsmöglichkeiten		<input type="checkbox"/>

Anlage 2

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

Zum Zeitpunkt der Beauftragung genehmigt der Auftraggeber den Einsatz folgender Subunternehmer für die nachfolgend dargestellten Tätigkeiten:

Name/Firma	Anschrift	Serverstandort	Tätigkeit

oder

Zum Zeitpunkt der Beauftragung werden keine Subunternehmer eingesetzt.

oder

Zum Zeitpunkt der Beauftragung werden keine Subunternehmer genehmigt.

Anlage 3

Ort der Verarbeitung

Zustimmungserfordernis bei Verarbeitung im unsicheren Drittland

Die Verarbeitung der Daten durch den Auftragnehmer und die vom Auftraggeber genehmigten Unterauftragnehmer (**Anlage 2**) findet grundsätzlich ausschließlich in der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem solchen Land statt, für das ein Angemessenheitsbeschluss der Europäischen Kommission gem. Art. 45 DSGVO vorliegt. Jede Verlagerung der Verarbeitung in ein sonstiges Land („unsicheres Drittland“) bedarf der Zustimmung des Auftraggebers und darf zudem nur erfolgen, wenn die gesetzlichen Voraussetzungen für Datenübermittlungen in Drittländer nach den anwendbaren Datenschutzgesetzen erfüllt sind.

Verarbeitung durch Auftragnehmer im unsicheren Drittland

Wenn die Verarbeitung der Daten durch den Auftragnehmer ausschließlich oder auch in einem unsicheren Drittland erfolgt, gelten die mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 erlassenen EU-Standardvertragsklauseln („EU-Standardvertragsklauseln 2021“).

Bei der Dokumentation der Einhaltung der aus den EU-Standardvertragsklauseln 2021 resultierenden Verpflichtungen werden Auftraggeber und Auftragnehmer eng zusammenarbeiten. Zur Erfüllung der in Klausel 14 der EU-Standardvertragsklauseln 2021 genannten Kriterien ist der Auftragnehmer verpflichtet, dem Auftraggeber alle insoweit erforderlichen Informationen zur Verfügung zu stellen. Der Auftragnehmer wird dem Auftraggeber insbesondere Fragen wahrheitsgemäß, umfassend und innerhalb eines angemessenen Zeitraums beantworten, die die Anwendbarkeit von Rechtsvorschriften und Gepflogenheiten bzw. deren praktische Umsetzung in den relevanten unsicheren Drittländern betreffen.

Wenn aufgrund der Rechtsvorschriften und Gepflogenheiten in diesen unsicheren Drittländern und angesichts der besonderen Umstände der Verarbeitung keine hinreichende Gewähr dafür besteht, dass die Verarbeitung im Einklang mit den EU-Standardvertragsklauseln 2021 erfolgt, wird der Auftragnehmer in Abstimmung mit dem Auftraggeber

- (i) zusätzliche technische und organisatorische Maßnahmen ergreifen und/oder
- (ii) zusätzliche vertragliche Zusicherungen abgeben, die unter Berücksichtigung dieser Rechtsvorschriften und Gepflogenheiten und der besonderen Umstände der Verarbeitung eine hinreichende Gewähr für die Verarbeitung der Daten unter Einhaltung der in den EU-Standardvertragsklauseln 2021 statuierten Pflichten des Auftragnehmers bieten („Zusätzliche Maßnahmen und Zusicherungen“).

Die Verarbeitung der Daten durch den Auftragnehmer darf erst dann beginnen, wenn die in Absatz 2 erwähnten Fragen des Auftraggebers durch den Auftragnehmer beantwortet

wurden und die nach Absatz 3 eventuell erforderlichen Zusätzlichen Maßnahmen und Zusicherungen ergriffen bzw. abgegeben wurden.

Verarbeitung durch Unterauftragnehmer im unsicheren Drittland (wenn Auftragnehmer in der EU ansässig ist).

Verarbeiten Unterauftragnehmer eines in der EU ansässigen Auftragnehmers Daten in einem unsicheren Drittland, stellt der Auftragnehmer in Ergänzung zu den genannten Voraussetzungen vor Beginn der Verarbeitung durch diese Unterauftragnehmer sicher, dass mit dem Unterauftragnehmer die EU-Standardvertragsklauseln 2021 abgeschlossen sind oder dass für den Unterauftragnehmer verbindliche interne Datenschutzvorschriften im Sinne von Art. 47 DSGVO gelten. Die unter Verarbeitung durch Auftragnehmer im unsicheren Drittland genannten Absätze 2 und 3 gelten entsprechend im Verhältnis zwischen Auftragnehmer und Unterauftragnehmer. Auf Verlangen des Auftraggebers stellt der Auftragnehmer diesem eine Kopie der insoweit relevanten Dokumente zur Verfügung.

Verarbeitung durch Unterauftragnehmer im unsicheren Drittland (wenn Auftragnehmer nicht in der EU ansässig ist)

Verarbeiten Unterauftragnehmer eines nicht in der EU ansässigen Auftragnehmers Daten in einem unsicheren Drittland, schließt der Auftragnehmer in Ergänzung zu den genannten Voraussetzungen vor Beginn der Verarbeitung durch diese Unterauftragnehmer mit diesen vertragliche Vereinbarungen, die in Bezug auf die Verarbeitung durch die Unterauftragnehmer sicherstellen, dass diese Verarbeitung auf einem Datenschutzniveau stattfindet, das dem durch die EU-Standardvertragsklauseln 2021 oder durch verbindliche interne Datenschutzvorschriften im Sinne von Art. 47 DSGVO gewährleisteten Niveau entspricht. Die unter Verarbeitung durch Auftragnehmer im unsicheren Drittland genannten Absätze 2 und 3 gelten entsprechend im Verhältnis zwischen Auftragnehmer und Unterauftragnehmer. Auf Verlangen des Auftraggebers stellt der Auftragnehmer diesem eine Kopie der insoweit relevanten Dokumente zur Verfügung.

Anlage 4

Änderungsmitteilung des bestehenden Vertrags zur Auftragsverarbeitung gemäß Art. 28 DSGVO für Auftragnehmer

Angaben zum Auftraggeber

Firmenname	
Adresse	

Angaben zum Auftragnehmer

Firmenname	
Adresse	

Mit dieser Änderungsmitteilung des bestehenden Vertrags zur Auftragsverarbeitung gemäß Art. 28 DSGVO, welche am geschlossen wurde, teilt der Auftragnehmer dem Auftraggeber folgende Vertragsänderung mit Wirksamkeit zum mit:

A. Änderung der Firmierung und/oder Adressangabe

Angaben zum Auftragnehmer

Firmenname (ALT)	
Firmenname (NEU)	
Adresse (ALT)	
Adresse (NEU)	

B. Änderung Vertragsgegenstand der Auftragsverarbeitung

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

.....

.....

.....

.....

C. Änderung Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

.....
.....
.....
.....

D. Änderung Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

.....
.....
.....
.....

E. Änderung der Verarbeitungstätigkeiten

Folgende Verarbeitungstätigkeiten sollen ausgeführt werden:

.....
.....
.....
.....

F. Änderung Ihrer technischen und organisatorischen Maßnahmen (Art. 32 DSGVO)

Bitte übermitteln Sie uns Ihre aktuelle Auflistung;
Alternativ: Folgende Änderungen haben sich ergeben:

.....
.....
.....
.....

G. Wechsel des Datenschutzbeauftragten / Ansprechpartners zum Datenschutz

Name, Vorname	
Organisationseinheit Firmenname, Adresse	
Telefon	
E-Mail	

H. Änderung der Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Bitte übermitteln Sie uns Ihre aktuelle Auflistung;

Alternativ: Folgende Änderungen haben sich ergeben:

Unterauftragnehmer (Firmenname, Adresse)	Art der Dienstleistung	Rechtsgrundlage nach Art. 44 ff. DSGVO für die Datenübermittlung in Drittstaaten

I. Änderung des Weisungsempfängers

Name, Vorname	
Abteilung	
Telefon	
E-Mail	

Ort, Datum

.....
Stempel u. Unterschrift
Auftragnehmer