

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO, als Anlage zum Hauptvertrag | zur Leistungsbeschreibung „xxx“ vom xxx

zwischen

Germany Trade & Invest

Gesellschaft für Außenwirtschaft und Standortmarketing mbH

Friedrichstraße 60

10117 Berlin

- nachstehend „Auftraggeber“ genannt

und

Name des Auftragnehmers

Straße und Nummer

Postleitzahl und Ort

- nachstehend „Auftragnehmer“ genannt

Präambel

Im Rahmen der Leistungserbringung nach o.g. Hauptvertrag / Leistungsbeschreibung ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt).

Dieser Vertrag konkretisiert die Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags / der Leistungsbeschreibung.

§ 1 Umfang der Beauftragung

- (1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers i. S. v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinne.
- (2) Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert. Die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages/den Regelungen in der Leistungsbeschreibung.

- (3) Jede von den Festlegungen in Anlage 1 abweichende oder darüberhinausgehende Verarbeitung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verarbeitung der Auftraggeber-Daten zu eigenen Zwecken. Das gilt auch für eine Anonymisierung der Auftraggeber-Daten und für jegliche Verwendung anonymisierter Auftraggeber-Daten.
- (4) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich im Gebiet der Bundesrepublik Deutschland (BRD), der Europäischen Union (EU) oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Datenverwendung in Ländern, die weder Mitgliedsstaat der EU noch Vertragsstaat des EWR sind (nachfolgend „Drittländer“ genannt) dürfen nur dann erfolgen, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber seine schriftliche Zustimmung vorab erteilt hat.
- (5) Die Verarbeitung von Daten außerhalb der Betriebsräume des Auftragnehmers (z. B. in Rechenzentren, mobiles Arbeiten o.ä.) bedarf der Festlegung angemessener technischer und organisatorischer Maßnahmen für die jeweilige Verarbeitungssituation. Der Auftragnehmer hat gegenüber dem Auftraggeber nachzuweisen, dass notwendige Richtlinien vorhanden sind sowie regelmäßige Kontrollen durchgeführt werden.
- (6) Der Auftragnehmer erwirbt an den Auftraggeber-Daten keine Rechte. Auf Verlangen des Auftraggebers ist der Auftragnehmer auf die Herausgabe der Auftraggeber-Daten in einer für den Auftraggeber lesbaren und weiterverarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf die Auftraggeber-Daten und die dazugehörigen Datenträger sind ausgeschlossen.

§ 2 Weisungsbefugnisse des Auftraggebers

- (1) Der Auftragnehmer darf die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Der Auftraggeber besitzt gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang, Zweck und Verfahren der Verarbeitung von Auftraggeber-Daten. Die Weisungen des Auftraggebers sollen grundsätzlich in Schrift- oder Textform erfolgen. Bei Bedarf kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen jedoch einer unverzüglichen Bestätigung durch den in Anlage 2 genannten Weisungsberechtigten des Auftraggebers in Schrift- und Textform. Der Auftragnehmer ist verpflichtet, sämtliche Weisungen des Auftraggebers zu dokumentieren.
- (3) Weisungen sollen im Regelfall von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden. Der Auftragnehmer bestimmt Empfangsberechtigte für Weisungen des Auftraggebers. Die weisungsberechtigten Personen beim Auftraggeber sowie die empfangsberechtigten Personen beim Auftragnehmer sind in Anlage 2 benannt. In dringenden Fällen darf der Auftraggeber jedem anderen Beschäftigten des Auftragnehmers entsprechende Weisungen erteilen, sofern weder der Empfangsberechtigte noch sein Stellvertreter für den Auftraggeber erreichbar waren.
- (4) Der Auftraggeber wird dem Auftragnehmer einen Wechsel in der Person des Weisungsberechtigten oder des Stellvertreters möglichst frühzeitig anzeigen.

- (5) Ein Wechsel in der Person des Empfangsberechtigten oder des Stellvertreters bzw. deren dauerhafte Verhinderung hat der Auftragnehmer dem Auftraggeber möglichst frühzeitig schriftlich unter Benennung eines Vertreters mitzuteilen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die bestimmten Personen weiter als empfangsberechtigt für Weisungen des Auftraggebers.
- (6) Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.
- (7) Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten in Einklang mit den Bestimmungen dieses Vertrages und den Weisungen des Auftraggebers verarbeitet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeber-Daten umgehen, die Vorschriften der DSGVO und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind, Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er unverzüglich darauf hinzuweisen, Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber mit mindestens 14-tägiger Frist berechtigt, die Ausführung der Weisung bis zur Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.
- (8) Falls die Weisung, die gemäß Ziffer 2.2 und Anlage 1 dieses Vertrages getroffene Festlegungen ändert oder aufhebt, ist sie nur zulässig, wenn hierbei eine entsprechende neue schriftliche Festlegung nach Ziffer 2.2 erfolgt.

§ 3 Anforderungen an Personal und Systeme

- (1) Der Auftragnehmer gewährt Personen Zugriff auf Auftraggeber-Daten nur, soweit dies unmittelbar für die Erfüllung einer konkreten Aufgabe durch diese Person notwendig ist (Need-to-know-Prinzip). Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten in Schriftform zur Vertraulichkeit zu verpflichten und die Verpflichtung dem Auftraggeber auf ersten Anfordern nachzuweisen.
- (2) Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedsstaaten zur Verarbeitung verpflichtet.
- (3) Der Auftragnehmer gewährleistet, dass er nur solche Systeme für die Verarbeitung von Auftraggeber-Daten einsetzt, die dafür ausgelegt sind, den Datenschutz durch eine der Verarbeitungssituation angemessene technische Systemgestaltung zu unterstützen.

§ 4 Sicherheit der Verarbeitung

- (1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zum Schutz der Auftraggeber-Daten.
- (2) Der Auftragnehmer garantiert, vor Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die in Anlage 3 zu diesem Vertrag spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

- (3) Dem Auftragnehmer ist es gestattet, nach vorheriger schriftlicher Zustimmung des Auftraggebers alternative adäquate technische und organisatorische Maßnahmen umzusetzen, sofern das Sicherheitsniveau der in Anlage 3 festgelegten technischen und organisatorischen Maßnahmen nicht unterschritten wird.
- (4) Auf Weisung des Auftraggebers wird der Auftragnehmer darüberhinausgehende wirksame technische und organisatorische Maßnahmen umsetzen, wenn sich die in Anlage 3 des Vertrages bestimmten Maßnahmen als nicht ausreichend erwiesen haben oder wenn der technische Fortschritt dies erfordert. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 3 nicht (mehr) ausreichend sind oder der technische Fortschritt weitere Maßnahmen erfordert.
- (5) Für die Sicherheit der Auftraggeber-Daten relevante Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind in jedem Fall vom Auftragnehmer im Voraus mit dem Auftraggeber abzustimmen, auch wenn hierdurch keine Abweichung von den Maßnahmen nach Anlage 3 erfolgt.
- (6) Auf Verlangen weist der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 3 festgelegten technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis durch die Vorlage eines aktuellen Testats oder Berichts einer unabhängigen Instanz (bspw. Wirtschaftsprüfer, Revision, betriebliche oder externe Datenschutzbeauftragte, etc.) oder einer geeigneten Zertifizierung (bspw. BSI-Grundschutz, etc.) erbracht werden. Die Kontrollrechte des Auftraggebers nach Ziffer 10 dieses Vertrages bleiben davon unberührt.
- (7) Der Auftragnehmer ist verpflichtet, die Grundsätze der ordnungsgemäßen automatisierten Verarbeitung personenbezogener Daten einzuhalten und insbesondere jeweils aktuelle Dokumentationen aller automatisierten Verfahren zur Verarbeitung von Auftraggeber-Daten vorzuhalten sowie definierte und dokumentierte Test- und Freigabeverfahren für diese automatisierte Verfahren einzuhalten.
- (8) Auf Verlangen stellt der Auftragnehmer dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung nach diesem Vertrag zur Verfügung.

§ 5 Inanspruchnahme weiterer Auftragsverarbeiter

- (1) Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer. Die gegenwärtig vom Auftragnehmer eingesetzten weiteren Auftragsverarbeiter sind in Anlage 4 genannt.
- (2) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter informieren. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung Einspruch zu erheben. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt. Im Falle zugelassener Änderungen wird der Auftragnehmer die Liste der Unterauftragnehmer in Anlage 4 aktualisieren und dem Auftraggeber unverlangt zur Verfügung stellen.
- (3) Der Auftragnehmer wird jeden weiteren Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in dieser Anlage in Bezug auf den Auftragnehmer festgelegt sind. In dem Unterauftragsverarbeitungsvertrag sind die Verantwortlichkeitssphären des

Auftragnehmers und des Weiteren Auftragsverarbeiters klar voneinander abzugrenzen. Der Auftragnehmer haftet für das Verschulden jedes weiteren Auftragsverarbeiters wie für eigenes Verhalten.

- (4) Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

§ 6 Rechte der betroffenen Personen

- (1) Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anfragen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
- (2) Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich spätestens aber innerhalb von 3 Tagen an den Auftraggeber weiterleiten und ohne entsprechende Einzelanweisung des Auftraggebers nicht mit der betreffenden Person in Kontakt treten.
- (3) Der Auftragnehmer wird dem Auftraggeber unverzüglich, längstens aber innerhalb von 5 Werktagen Informationen über die gespeicherten Auftraggeber-Daten (auch soweit sie sich auf den Speicherungszweck beziehen), die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen.
- (4) Der Auftragnehmer ist verpflichtet, Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich, spätestens aber innerhalb einer Frist von 5 Werktagen, zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. Der Auftragnehmer wird dem Auftraggeber die weisungsgemäße Berichtigung oder Löschung der Daten bzw. die Einschränkung von deren Verarbeitung jeweils auf Verlangen schriftlich bestätigen.
- (5) Der Auftragnehmer stellt sicher, dass er auf Einzelweisung des Auftraggebers den gesamten zu einer Person gespeicherten Datensatz in einem vom Auftraggeber im Einzelfall festzulegenden, strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber übergeben kann.

§ 7 Mitteilungs- und Unterstützungspflichten bei Verletzung des Schutzes von Auftraggeber-Daten

- (1) Der Auftragnehmer meldet dem Auftraggeber unverzüglich – spätestens aber innerhalb von 24 Stunden – nachdem ihm eine solche bekannt geworden ist, jede potentielle Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugtem Zugang zu Auftraggeber-Daten führen können („Datensicherheitsvorfall“). Die Meldung enthält mindestens eine Beschreibung:

- der Art der Verletzung des Schutzes der Auftraggeber-Daten mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - der möglichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;
 - der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (2) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach Art. 33 oder Art. 34 DSGVO) auf erstes Auffordern im Rahmen des Zumutbaren zu unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.
- (3) Der Auftragnehmer ist verpflichtet, unverzüglich nach Kenntniserlangung von einem Datensicherheitsvorfall eine Ursachenanalyse (Root-Cause-Analyse, RCA) durchzuführen, diese zu dokumentieren und dem Auftraggeber die Dokumentation auf Verlangen auszuhändigen. Stellt der Auftragnehmer hierbei fest, dass die bisherigen vom Auftragnehmer realisierten technischen und organisatorischen Maßnahmen zum Schutz der Auftraggeber-Daten nicht ausreichend waren, ist der Auftragnehmer verpflichtet, ohne zusätzliche Kosten solche zusätzlichen technischen und organisatorischen Maßnahmen umzusetzen, die nach Ansicht des Auftraggebers erforderlich sind für einen angemessenen Schutz der Auftraggeber-Daten gegen Datensicherheitsvorfälle.
- (4) Der Auftragnehmer ist verpflichtet, ein Verzeichnis über alle sich während der Vertragslaufzeit bei ihm ereignenden Datensicherheitsvorfälle zu führen, in das Informationen aufzunehmen sind über
1. sämtliche Umstände und Fakten im Zusammenhang mit dem Datensicherheitsvorfall,
 2. dessen Auswirkungen und Auswirkungen und
 3. den jeweils ergriffenen Abhilfemaßnahmen.
- Auf Verlangen des Auftraggebers hat der Auftragnehmer ihm dieses Verzeichnis vorzulegen.

§ 8 Sonstige Unterstützungspflichten des Auftragnehmers

- (1) Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, wenn das Eigentum des Auftraggebers oder seine sonstigen Rechte an den Auftraggeber-Daten beim Auftragnehmer durch Maßnahmen dritter, z.B. durch Pfändung, Beschlagnahme, Insolvenz oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird. Ferner wird der Auftragnehmer alle jeweils beteiligten Dritten darüber informieren, dass die Auftraggeber-Daten im Eigentum des Auftraggebers stehen.
- (2) Ist der Auftraggeber gegenüber einer staatlichen Stelle oder einem Dritten verpflichtet, Auskünfte über die Auftraggeber-Daten oder deren Verarbeitung zu erteilen, so ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erteilung solcher Auskünfte auf erstes Anfordern zu unterstützen, insbesondere durch unverzügliche Zurverfügungstellung sämtlicher Informationen und Dokumente über die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten einschließlich

der vom Auftragnehmer ergriffenen technisch-organisatorischen Maßnahmen, über den technischen Ablauf und die Orte der Verarbeitung von Auftraggeber-Daten und über die an der Verarbeitung beteiligten Personen.

- (3) Der Auftragnehmer hat dem Auftraggeber auf Verlangen unverzüglich eine jeweils aktuelle Aufstellung der Angaben nach Art. 30 Abs. 2 DSGVO sowie die beim Auftragnehmer zugriffsberechtigten Personen jeweils in Bezug auf die Auftraggeber-Daten zur Verfügung zu stellen.
- (4) Der Auftragnehmer bestätigt, dass er einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DSGVO bestellt hat und verpflichtet sich, die Bestellung eines Datenschutzbeauftragten während der Dauer der Verarbeitung von Auftraggeber-Daten aufrechtzuerhalten, auch wenn die gesetzlichen Voraussetzungen für eine Bestellpflicht entfallen sind. Die Kontaktdaten des Datenschutzbeauftragten sind in **Anlage 2** zu ergänzen. Einen Wechsel in der Person des Datenschutzbeauftragten hat der Auftragnehmer dem Auftraggeber unverzüglich schriftlich mitzuteilen.
- (5) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei etwa von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

§ 9 Datenlöschung und -rückgabe

- (1) Der Auftragnehmer wird auf Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages/Leistungsbeschreibung alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung des Auftraggeber-Daten besteht.
- (2) Der Auftragnehmer stellt darüber hinaus sicher, dass er Auftraggeber-Daten auf Einzelanweisung des Auftraggebers jederzeit löschen kann, etwa, wenn ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Verarbeitung nicht mehr erforderlich ist.
- (3) Die Bestimmungen der Ziffern 11.1 und 11.2 gelten auch für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie für Test- und Ausschussdaten.
- (4) Über jede Löschung und Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein schriftliches Protokoll zu erstellen, das dem Auftraggeber nach Beendigung des Auftrages vorzulegen ist.

§ 10 Nachweise und Überprüfungen

- (1) Der Auftragnehmer hat sicherzustellen und regelmäßig (mindestens einmal pro Jahr) zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit diesem Vertrag sowie den Weisungen des Auftraggebers im Einklang stehen.
- (2) Der Auftragnehmer wird die Umsetzung der Pflichten nach diesem Vertrag in geeigneter Weise dokumentieren und dem Auftraggeber entsprechende Nachweise auf dessen Verlangen vorlegen. Der Auftragnehmer wird insbesondere dokumentieren:
 - alle Eigenkontrollen gemäß Ziffer 10.1
 - alle Vertraulichkeitsverpflichtungen von Personen, die Auftraggeber-Daten verarbeiten

- alle Verträge über die Inanspruchnahme weiterer Auftragsverarbeiter und alle Prüfungen weiterer Auftragsverarbeiter im Sinne von Ziffer 7
 - alle auf Weisung des Auftraggebers erfolgten Löschungen von Auftraggeber-Daten
- (3) Der Auftraggeber ist berechtigt, den Auftragnehmer regelmäßig während der Verarbeitung von Auftraggeber-Daten bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Anlage 3** zu überprüfen, einschließlich durch Vor-Ort-Kontrollen, die rechtzeitig anzumelden sind.
- (4) Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch die Bereitstellung aller notwendigen Informationen einschließlich Zertifikate, Auditberichte und sonstige Ergebnisse von Überprüfungen im Hinblick auf die Verarbeitung von Auftraggeber-Daten.
- (5) Der Auftraggeber ist berechtigt, von dem Datenschutzbeauftragten des Auftragnehmers Auskunft über sämtliche Aspekte der Verarbeitung von Auftraggeber-Daten, einschließlich der getroffenen technischen und organisatorischen Maßnahmen, zu erhalten und von ihm regelmäßig eine Bestätigung der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 3** zu verlangen. Der Auftragnehmer wird unter Beachtung von dessen Weisungsfreiheit dafür sorgen, dass der Datenschutzbeauftragte auf Verlangen des Auftraggebers Auskünfte und Bestätigungen zeitnah erteilt.
- (6) Der Auftraggeber ist berechtigt, die Kontrollhandlungen nach dieser Ziffer 12 selbst oder durch einen zur Geheimhaltung verpflichteten Bevollmächtigten vorzunehmen. Der Auftragnehmer ist verpflichtet die Kontrollhandlungen eines solchen Bevollmächtigten in derselben Weise zu dulden und zu unterstützen wie Kontrollen durch den Auftraggeber.

§ 11 Vertragsdauer und Kündigung

- (1) Die Laufzeit des Vertrages entspricht der Laufzeit des Hauptvertrages bzw. der Angaben in der Leistungsbeschreibung. Die Regelungen zur ordentlichen Kündigung des Hauptvertrages gelten entsprechend.
- (2) Der Auftraggeber ist zu einer jederzeitigen außerordentlichen Kündigung dieses Vertrages sowie des Hauptvertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt für den Auftraggeber insbesondere dann vor, wenn
- der Auftragnehmer gegen wesentliche Pflichten aus diesem Vertrag verstößt;
 - der Auftragnehmer die Auftraggeber-Daten für andere als nach Ziffer 2.2 zugelassene Zwecke verwendet;
 - Der Auftragnehmer eine Weisung des Auftraggebers nach Ziffer 1 dieses Vertrages nicht ausführt;
 - Der Auftragnehmer einer Meldepflicht nach Ziffer 7.1 nicht nachkommt;
 - Der Auftragnehmer der Ausführung der Kontrollpflichten nach Ziffer 9 dieses Vertrages verweigert oder nicht nur unerheblich behindert oder
 - Der Auftragnehmer einen weiteren Auftragsverarbeiter entgegen Ziffer 7.1 ohne vorherige schriftliche Zustimmung des Auftraggebers einschaltet.

- (3) Der Hauptvertrag darf im Falle einer Beendigung dieses Vertrages nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragnehmer Auftraggeber-Daten verarbeitet. Im Zweifel gilt eine Kündigung des Hauptvertrages auch als eine Kündigung dieses Vertrages und gilt eine Kündigung dieses Vertrages auch als Kündigung des Hauptvertrages.

§ 12 Haftung

- (1) Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend der gesetzlichen Haftungsregelungen. Etwaige anderweitig zwischen den Parteien vereinbarte Haftungsregelungen (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen diesen Vertrag oder gegen ein ihn unmittelbar treffende gesetzliche Datenschutzverpflichtung haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf erstes Anfordern frei.
- (2) Der Auftragnehmer verpflichtet sich, den Auftraggeber auch von allen etwaigen Geldbußen, die gegen den Auftraggeber verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftragnehmer Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.
- (3) Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden und Geldbußen nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die jeweilige Ursache in der Verarbeitung von Auftraggeber-Daten in der Zuständigkeitssphäre des Auftragnehmers liegt.

§ 13 Schlussbestimmungen

- (1) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Regelungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.
- (2) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gegen die Regelungen dieses Vertrages vor.
- (3) Jede Änderung dieses Vertrages bedarf einer ausdrücklichen Vereinbarung zwischen den Parteien.

Name des Unternehmens

Ort, den Datum

Auftragnehmer | zusätzlich eingescannte Unterschrift

Germany Trade & Invest GmbH

Berlin, den

Anlagen:

- Anlage 1: Leistungsbeschreibung der Auftragsverarbeitung
- Anlage 2: Weisungsberechtigte Personen beim Auftraggeber. Empfangsberechtigte Personen beim Auftragnehmer. Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers
- Anlage 3: Technische und organisatorische Maßnahmen
- Anlage 4: Weitere Auftragsverarbeiter

Anlage 1

Leistungsbeschreibung der Auftragsverarbeitung

A. Zweck der Datenverarbeitung

Der Zweck ergibt sich aus der Aufgabe, zu deren Erfüllung die personenbezogenen Daten des Auftraggebers verarbeitet werden.

[Hier eingeben]

B. Art und Umfang der Datenverarbeitung

Kurze inhaltliche Beschreibung der zu Erfüllenden Dienstleistung.

[Hier eingeben]

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

Zutreffendes bitte ankreuzen

- ☐ Personenstammdaten: Name
- ☐ Kommunikationsdaten: Telefonnummer, E-Mailadresse
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- und Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. von Auskunftseien oder öffentliche Verzeichnisse)
- ☐ Sonstige: [Hier eingeben]

D. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Zutreffendes bitte ankreuzen

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter

☐ Ansprechpartner

☐ Sonstige: [Hier eingeben]

Anlage 2

A. Weisungsberechtigte Person des Auftraggebers

Weisungsberechtigte Person:

[Hier eingeben]

Stellvertretung:

[Hier eingeben]

B. Empfangsberechtigte Person für Weisungen beim Auftragnehmer

Empfangsberechtigte Person:

[Hier eingeben]

Stellvertretung:

[Hier eingeben]

C. Kontaktdaten des Datenschutzbeauftragten

Name und Kontaktdaten des Datenschutzbeauftragten:

[Hier eingeben]

Name und Kontaktdaten des Ansprechpartners für Datenschutz, sofern kein Datenschutzbeauftragter bestellt:

[Hier eingeben]

Anlage 3

Technische und organisatorische Maßnahmen

I. Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

II. Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

III. Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

☐ Schlüssel	☐ Magnet- oder Chipkarte
☐ elektrische Türöffner	☐ Werkschutz, Pfortner
☐ Alarmanlage	☐ Sonstiges: [Hier eingeben]

Zugangskontrolle

Keine unbefugte Systembenutzung

☐ Authentifikation mit Benutzername Passwort	☐ 2-Faktor-Authentifizierung
☐ Einsatz von passwortgeschützten Bildschirmschonern	☐ Firewall

☐ Verschlüsselung von (mobilen) Datenträgern	☐ Antiviren Software
☐ Einsatz von Angriffserkennungssystemen (Intrusion Detection)	☐ Sonstiges: [Hier eingeben]

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

☐ Verwaltung von Berechtigungskonzepten	☐ Need to know Prinzip
☐ Protokollierung von Zugriffen	☐ Einsatz von Aktenvernichtern
☐ sichere Aufbewahrung von Datenträgern	☐ Löschung von Daten nach Ablauf der Aufbewahrungsfristen
☐ Sonstiges: [Hier eingeben]	

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

☐ Mandantenfähigkeit	☐ Berechtigungskonzepte (Funktions- und Datenebene)
☐ physikalisch getrennte Speicherung auf Systemen, Datenträgern und Ordnern	☐ Sonstiges: [Hier eingeben]

2. 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 Person zugeordnet werden können. Die zusätzlichen Informationen werden gesondert aufbewahrt und durch angemessene technische und organisatorische Maßnahmen geschützt.

☐ Pseudonymisierung wird vorgenommen		☐ Ersetzung durch Kennzeichen ☐ Zugriffsgeschützte Kennzeichenaufbewahrung
☐ Pseudonymisierung wird nicht vorgenommen		Begründung: [Hier eingeben]

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

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

☐ Transportverschlüsselung beim E-Mail-Versand (TLS)	☐ elektronische Signatur
☐ Einsatz von Virtual Private Network (VPN)	☐ Sonstiges: [Hier eingeben]

Eingabekontrolle

Feststellung, ob und wann personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges: [Hier eingeben]	

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

☐ Vorhandensein eines Backup- und Recovery-Konzeptes	☐ Unterbrechungsfreie Stromversorgung (USV)
☐ sichere, räumlich getrennte Lagerung von Sicherungsmedien	☐ Meldewege und Notfallpläne dokumentiert
☐ Sonstiges: [Hier eingeben]	

☐ Rasche Wiederherstellbarkeit gewährleistet (Art. 32 Abs. 1 lit. c DSGVO)

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

☐ regelmäßige Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen	☐ Bestellung Datenschutzbeauftragte bei Bestellopflicht bzw. Benennung eines internen Ansprechpartners für Datenschutz
☐ Datenschutzschulungen für Beschäftigte	☐ Prüfung der internen Verfahren auf Datenschutzkonformität

☐ Umsetzung von datenschutz-freundlichen Voreinstellungen in IT-Systemen	☐ Maßnahmen zur Abwehr und schnellen Eindämmung von Cybervorfällen (Incident Response)
☐ sorgfältige Auswahl von Auftragsverarbeitern u. a. hinsichtlich der implementierten technischen und organisatorischen Maßnahmen	☐ schriftliche Regelung der Auftragsverarbeitung (Auftragsverarbeitungsvertrag)
☐ Kontrolle der Auftragsverarbeiter	☐ Sonstiges: [Hier eingeben]

IV. Ergänzende beigefügte Unterlagen

Zusätzlich zu den Angaben unter Ziffer III. werden folgende Unterlagen beigefügt:

- ☐ IT-Sicherheitskonzept, ggf. abweichende Bezeichnung [Hier eingeben]
- ☐ Datenschutzkonzept, ggf. abweichende Bezeichnung [Hier eingeben]
- ☐ Datenschutz- und Sicherheitshandbuch, ggf. abweichende Bezeichnung [Hier eingeben]
- ☐ Zertifizierungen, welche: [Hier eingeben]
- ☐ Prüf- bzw. Auditberichte interner Datenschutzkontrollen, konkrete Bezeichnung [Hier eingeben]
- ☐ kundenspezifisches Löschkonzept, ggf. abweichende Bezeichnung [Hier eingeben]
- ☐ Weitere Unterlagen: [Hier eingeben]

Anlage 4

Weitere Auftragsverarbeiter

Die vertraglich vereinbarte Leistung bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Unterauftragsverarbeiter durchgeführt:

- ☐ Es wird bestätigt, dass die nachfolgend genannten Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen von uns sorgfältig ausgewählt wurden und wir uns von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugt haben.

Firma Anschrift	Beschreibung der Teilleistung	Ort der Verarbeitung	Angaben zu geeigneten Garantien bei Daten- übermittlung in ein Drittland	Ansprechpartner Datenschutz
[Hier eingeben]	[Hier eingeben]	☐ BRD ☐ EU/EWR ☐ Drittland: [Hier eingeben]	[Hier eingeben]	[Hier eingeben]
[Hier eingeben]	[Hier eingeben]	☐ BRD ☐ EU/EWR ☐ Drittland: [Hier eingeben]	[Hier eingeben]	[Hier eingeben]
[Hier eingeben]	[Hier eingeben]	☐ BRD ☐ EU/EWR ☐ Drittland: [Hier eingeben]	[Hier eingeben]	[Hier eingeben]
[Hier eingeben]	[Hier eingeben]	☐ BRD ☐ EU/EWR ☐ Drittland: [Hier eingeben]	[Hier eingeben]	[Hier eingeben]