

Vereinbarung zur Verarbeitung von Daten im Auftrag

zwischen

items GmbH & Co. KG
Hafenweg 7
48155 Münster

– Auftraggeber –

und

Daten Auftragnehmer

– Auftragnehmer –

beide gemeinsam auch als Vertragspartner bezeichnet.

1. ALLGEMEINES

(1) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragspartner im Umgang mit Auftraggeberdaten bzw. Daten eines Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO, für welchen wiederum der Auftraggeber Auftragsverarbeiter ist. Sie findet Anwendung auf alle Tätigkeiten, die mit den Verträgen in Zusammenhang stehen und bei denen Mitarbeiter der Auftragnehmerin oder durch die Auftragnehmerin beauftragte Dritte mit personenbezogenen Daten der Auftraggeberin bzw. Daten eines Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO, für welchen wiederum der Auftraggeber Auftragsverarbeiter ist in Berührung kommen können. Dies gilt insbesondere im Hinblick auf den zu gewährleistenden Schutz bei der Verarbeitung personenbezogener Daten im Sinne von Art. 28 Datenschutzgrundverordnung (DSGVO) (im Folgenden: „Auftragsverarbeitung“) durch den Auftragnehmer oder von ihm unterbeauftragten Dritten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Der Verantwortliche, für den der Auftraggeber (items) als Auftragsverarbeiter tätig wird, wird im Folgenden als Hauptauftraggeber bezeichnet.

2. GEGENSTAND DES AUFTRAGS

(1) Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

(2) Mit diesem Vertrag werden etwaige zwischen den Vertragspartnern bestehende Verträge zur Auftragsverarbeitung aufgehoben.

3. RECHTE UND PFLICHTEN DES AUFTRAGGEBERS

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber bzw. der Hauptauftraggeber bleibt auch bei der Auftragsverarbeitung weiterhin allein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. ALLGEMEINE PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine

Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail) erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 – 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. MELDEPFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber bzw. den Hauptauftraggeber, eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bzw. den Hauptauftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. MITWIRKUNGSPFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer unterstützt den Auftraggeber bzw. den Hauptauftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bzw. den Hauptauftraggeber, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. „HOME-OFFICE“-REGELUNG

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, mit vorheriger Zustimmung des Auftraggebers die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben. Die Zustimmung des Auftraggebers bedarf der Textform (z.B. E-Mail).

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office“ eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. KONTROLLBEFUGNISSE

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle im „Home-Office“ von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. UNTERAUFTRAGSVERHÄLTNISSE

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11. VERPFLICHTUNG AUF DIE VERTRAULICHKEIT

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie

sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

(4) Soweit der Auftragnehmer für den Auftraggeber im Rahmen der Tätigkeit bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er zur Wahrung des Fernmeldegeheimnisses verpflichtet.

12. WAHRUNG VON BETROFFENENRECHTEN

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser bzw., der Hauptauftraggeber, insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

(4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber bzw. der Hauptauftraggeber, verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber bzw. der Hauptauftraggeber, der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

13. GEHEIMHALTUNGSPFLICHTEN

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

14. VERGÜTUNG

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

15. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

16. DAUER DES AUFTRAGS

(1) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

17. BEENDIGUNG

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

18. ZURÜCKBEHALTUNGSRECHT

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

19. SCHLUSSBESTIMMUNGEN

(1) Sollte das Eigentum des Auftraggebers bzw. des Hauptauftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den _____
Ort Datum

_____, den _____
Ort Datum

- Auftraggeber -

- Auftragnehmer -

ANLAGE 1 - GEGENSTAND DES AUFTRAGS

1. GEGENSTAND UND ZWECK DER VERARBEITUNG

Die Auftraggeberin beauftragt die Auftragnehmerin mit der ordnungsgemäßen und datenschutzgerechten Erbringung insbesondere folgender Leistungen:

Die vom Auftragnehmer zu erbringenden Leistungen sollen hier möglichst konkret beschrieben werden. Auch der Zweck der Verarbeitung ist zu benennen, sofern sich dies nicht aus der Leistungsbeschreibung ergibt.

Z.B. Hosting, Wartung/Support etc.

2. ART(EN) DER PERSONENBEZOGENEN DATEN

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Hier sollten die Datenfelder nach Möglichkeit konkret angegeben werden. Wenn dies nicht abschließend möglich ist, sind Generalisierungen erlaubt (Nutzungsdaten, Bestandsdaten etc.) und, soweit wie möglich zu konkretisieren.

Z.B. Verbrauchsdaten, Zählernummern, Bankdaten etc.

3. KATEGORIEN BETROFFENER PERSON

Kreis der von der Datenverarbeitung betroffenen Personen:

z.B. Kunden, Auftraggeber, Dritte etc.

ANLAGE 2 - UNTERAUFTRAGNEHMER

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Hier sind alle Unternehmen mit Namen, Rechtsform, Kontaktdaten und ladungsfähiger Anschrift vom Auftragnehmer anzugeben. Ferner ist die Art der Leistung kurz zu beschreiben.

ANLAGE 3 - MINDESTANFORDERUNGEN TECHNISCHER UND ORGANISATORISCHER MAßNAHMEN FÜR DEN AUFTRAGNEHMER

Die Verpflichtung von Auftragnehmern auf die Vertraulichkeit und die Einhaltung von Mindestanforderungen im Bereich der Informationssicherheit und des Datenschutzes soll einen angemessenen Schutz der Informationswerte des Auftraggebers gewährleisten. Dabei wird ein Mindestniveau von Schutzmaßnahmen festgeschrieben, welches von jedem Auftragnehmer im Hinblick auf dessen IT-Systeme und Prozesse zu erfüllen ist.

Die vom Auftragnehmer umzusetzenden technischen und organisatorischen Maßnahmen ergeben sich aus:

- den für die konkrete Leistung jeweils relevanten Vertrag im Rahmen der Geschäftsbeziehung geschlossenen Vertrag (Hauptvertrag) einschließlich sämtlicher Anlagen (bspw. Leistungsbeschreibungen) und ergänzend
- den nachfolgend aufgeführten technischen und organisatorischen Maßnahmen.

Die folgenden Mindestanforderungen sind von allen Auftragnehmern einzuhalten, die Zugriff auf Informationen und personenbezogene Daten des Auftraggebers erhalten; weitergehende oder zusätzliche Maßnahmen, die im Hauptvertrag oder dessen Anlagen festgelegt sind, sind ebenfalls verbindlich umzusetzen. Diese Anforderungen bilden einen integralen Bestandteil des Vertragsverhältnisses. Bei Widersprüchen haben die Regelungen des Hauptvertrags einschließlich seiner Anlagen Vorrang vor den nachfolgend aufgeführten Maßnahmen.

Der Auftraggeber ist berechtigt, die Einhaltung der Maßnahmen zu überprüfen.

Zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber kann der Auftraggeber auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach ISO/IEC 27001) anfordern.

1. ÜBERSICHT UND ANWENDUNGSBEREICH

Die hier beschriebenen technischen und organisatorischen Maßnahmen gelten als Mindest-Standard und dürfen nicht unterschritten werden. Sie gelten abhängig vom Zugriffs- oder Verarbeitungstyp (A–C):

Zugriffs- und Verarbeitungstyp	Beschreibung
A	Verarbeitung auf Systemen des Auftragnehmers (z. B. Cloud, Hosting, Outsourcing)
B	Zugriff des Auftragnehmers mit eigenen Endgeräten auf Systeme des Auftraggebers
C	Verwendung von Endgeräten und Systemen des Auftraggebers

2. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Kategorie	Beschreibung der Maßnahmen	gilt für
Organisation des Datenschutzes und der Informationssicherheit	Es bestehen klare Verantwortlichkeiten für Datenschutz und Informationssicherheit (ISB, DSB). Richtlinien und Prozesse sind dokumentiert, kommuniziert und werden regelmäßig überprüft.	A
	Sicherheitskonzepte und -maßnahmen sind implementiert und werden regelmäßig überprüft.	A, B
	Alle Mitarbeitenden und eingesetzte Unterauftragnehmer sind auf die Vertraulichkeit verpflichtet und werden regelmäßig geschult.	A - C
Physische Sicherheit und Zutrittschutz	Es sind physische Sicherheitskontrollen für Büros, Räume und Einrichtungen konzipiert und umgesetzt. Sicherheitsmaßnahmen und Zutrittsrechte entsprechend den jeweiligen Sicherheitsanforderungen. Es existiert ein dokumentiertes Verfahren zur Vergabe, Änderung und zum Entzug von Zutrittsrechten einschließlich der Rückgabe von Zutrittsmitteln.	A - C
	In Rechenzentren sind Schutzmaßnahmen gegen technische Beeinträchtigungen und Elementarschäden umgesetzt (u.a. USV, Klimaanlage, Schutz gegen Feuer und Wasser). Der Zutritt zu Rechenzentren ist auf den autorisierten Personenkreis beschränkt. Besucher werden begleitet und mit Datum und Uhrzeit Ihres Betretens und Verlassens erfasst. Es sind wirksame Zutrittsschutzmaßnahmen umgesetzt, einschließlich personengebundener, sicherer Zutrittsmittel, der Überwachung und Protokollierung von Zutritten sowie ein effektiver Einbruchschutz (EMA und VÜ).	A

Zugangs- und Zugriffssteuerung	Die Vergabe, Änderung und Genehmigung von Zugangs- und Zugriffsrechten unterliegen klar definierten Prozessen. Systemzugänge werden ausschließlich über personalisierte Konten bereitgestellt. Die Vergabe von Zugriffsrechten erfolgt nach dem „Need-to-Know“ und „least-privilege“ Prinzip. Accounts und Zugriffsrechte werden regelmäßig überprüft, inaktive Konten unverzüglich gesperrt, nicht erforderliche Zugriffe entzogen. Passwortvorgaben und Authentifizierungsverfahren entsprechen aktuellen Sicherheitsstandards. Privilegierte Konten (z.B. Systemadministratoren) werden durch starke Authentifizierung (z.B. MFA) geschützt, sind auf ein Minimum zu beschränken und werden streng überwacht. Administrator-Accounts dürfen nicht für normale Bürotätigkeiten verwendet werden.	A
	Arbeitsplätze sind durch automatische Bildschirmsperren zu schützen. Systemzugänge werden entweder gesichert oder gesperrt.	A, B
Verschlüsselung	Mobile Endgeräte werden entsprechend dem Stand der Technik verschlüsselt.	A, B
	Eine Datenübertragung über öffentliche Netze oder anderweitig nicht vertrauenswürdige Netze erfolgt ausschließlich über verschlüsselte Verbindungen (TLS, VPN).	A, B
Transport und Entsorgung von Datenträgern	Externe elektronische Medien (bspw. tragbare Festplatten, Band, USB-Sticks) werden bei Transporten außerhalb des Bereiches des Auftragnehmers in gesicherten, verschlossenen Transportbehältnissen durch spezielle Kurierdienste transportiert oder durch Verfahren wie Verschlüsselung gesichert. Bei der Datenlöschung und Vernichtung von Datenträgern sind die Vorgaben der ISO 21964 einzuhalten.	A

System- und Betriebssicherheit	Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-Audits, CVS-Datenbank) und bewertet (z. B. Common Vulnerability Scoring System CVSS). Potenziell betroffene IT-Systeme und Software werden identifiziert, beurteilt und Schwachstellen behandelt. Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) werden regelmäßig auf bekannte Schwachstellen hin analysiert. Aufgedeckte Schwachstellen und Ergebnisse werden in geeigneter Weise analysiert, klassifiziert und behoben. Abhilfemaßnahmen werden entsprechend ihrer Kritikalität zeitnah umgesetzt. Es existiert ein definierter Patch-Management-Prozess, der sicherstellt, dass auf der vom Auftragnehmer eingesetzten Hardware ausschließlich korrekt lizenzierte Software verwendet wird und alle Systeme regelmäßig mit aktuellen Sicherheits-Patches versorgt werden. Hardware (z. B. Clients, Server, Gateways), die zur Leistungserbringung eingesetzt wird, wird durch angemessene, aktuelle Anti-Malware-Software geschützt. Die Software erkennt, wenn der Schutz deaktiviert ist oder nicht regelmäßig aktualisiert wird. Bei Erkennung einer Bedrohung erfolgt eine automatisierte Alarmierung und eine angemessene, nachvollziehbare Bearbeitung. IT-Ressourcen (z. B. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) werden auf Basis sicherer Grundlagen (Härtung) konfiguriert und betrieben. Die Sicherheitsstandards orientieren sich an Best Practices, wie den CIS-Standards oder gleichwertigen Verfahren. Konfigurationen der IT-Anlagen werden regelmäßig überprüft und aktualisiert. Es werden risikobasierte Protokollierungs- und Überwachungsmaßnahmen etabliert, die relevante System-, Netzwerk- und Benutzeraktivitäten erfassen. Der Detailgrad richtet sich nach der Sensibilität der Information und der Systemkritikalität und ermöglicht die Nachvollziehbarkeit von Änderungen, auch an personenbezogenen Daten. Ereignisdaten aus Endgeräten und Netzwerkzonen werden zentral zusammengeführt und kontinuierlich auf Sicherheitsereignisse ausgewertet.	A, B
---------------------------------------	---	-------------

	Es existieren formale Richtlinien für das Change-Management und den Lebenszyklus der sicheren Softwareentwicklung, die sicherheitsrelevante Kontrollen festlegen. Sicherheitsüberprüfungen bei neuen Systemdesigns oder Änderungen sowie Sicherheitstests vor der Bereitstellung sind fester Bestandteil der Prozesse. Änderungen werden erst nach angemessener Anforderung, Autorisierung, Testung und Genehmigung für die Produktion freigegeben.	A
Trennungskontrolle	Umgebungen sind physisch oder logisch getrennt. Insbesondere bei gemeinsam mit anderen Auftraggebern genutzten Umgebungen sowie beim Betrieb von Test-, Qualitäts- und Produktionsumgebungen.	A
Netzwerksicherheit	Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen sind voneinander zu trennen (z. B. durch Firewalls). Netzwerkperimeter müssen durch Firewalls geschützt sein, und Firewallregeln einen dokumentierten Freigabeprozess durchlaufen. Authentisierungsmerkmale (z. B. Passwörter, PINs) werden ausschließlich verschlüsselt übertragen. Aus dem Internet erreichbare administrative Zugänge oder technische Netzwerkports sind abzuschalten oder angemessen abzusichern (z. B. mittels Zwei-Faktor-Authentisierung).	A
Backup und Wiederherstellung	Sicherungs- und Datenhaltungskonzepte für alle relevanten Plattformen und Komponenten im Verantwortungsbereich des Auftragnehmers sind implementiert und umgesetzt. Aufbewahrungsfristen sind definiert, Backups sowie Wiederherstellungstests werden nachweisbar durchgeführt. Die Sicherungskonzepte und Wiederherstellungsverfahren sind so ausgelegt, dass die vereinbarten Verfügbarkeitsstufen gewährleistet werden.	A
IT-Notfallmanagement	Notfallkonzepte und Wiederanlaufpläne sind dokumentiert, getestet und enthalten klare Rollen und Kommunikationswege.	A
Vorfallmanagement	Es existieren dokumentierte Verfahren für Informationssicherheits- und Datenschutzvorfälle, die eine wirksame und ordnungsgemäße Behandlung sicherstellen. Die Verfahren umfassen Meldung, Analyse, Überwachung, Lösung und Dokumentation von Vorfällen sowie Reaktions- und Wiederherstellungsprozesse. Datenschutzvorfälle und Vorfälle mit Auswirkungen auf die Leistungserbringung werden dem Auftraggeber unverzüglich gemeldet.	A, B

Lieferantenmanagement	Mit allen Unterauftragnehmern bestehen verbindliche Vereinbarungen, die ihre Verantwortung für die Sicherheit, der im Auftrag des Auftraggebers verarbeiteten, gespeicherten oder übermittelten Daten festlegen. Ihre Sicherheitsmaßnahmen müssen mindestens dem in diesem Dokument und im Hauptvertrag definierten Schutzniveau entsprechen. Einhaltung und Wirksamkeit werden im Rahmen des Lieferantenmanagements durch den Auftragnehmer regelmäßig überprüft.	A - C
-----------------------	---	-------