Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (AV-Vertrag)

Sie können dieses Dokument an die Bedürfnisse in Ihrem Verein anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass das DEUTSCHE EHRENAMT keinerlei Haftung übernimmt.

Hinweis: In einigen unserer Datenschutz-Vorlagen finden Sie Infoboxen dieser Art. Sie geben wichtige Hinweise darauf, wie bestimmte Aspekte zu handhaben sind. Sie können und sollten diese Boxen natürlich aus Ihrem angepassten Dokument entfernen.

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen_____ und_____

vertreten durch_____ vertreten durch_____

im Folgenden: **Auftraggeber**_____

im Folgenden: **Auftragnehmer**_____

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

Hinweis: In der Praxis überrascht immer wieder, wie oft Vereinbarungen zur Auftragsverarbeitung für eher unverbindliche „Datenschutzerklärungen" gehalten werden. Aus diesem Grund spricht dieses Muster konsequent von einem „Vertrag".

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche", der Auftragnehmer der „Auftragsverarbeiter". Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen: [BESCHREIBUNG]
Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag XYZ (im Folgenden „Hauptvertrag").

2.2 Dauer

Die Verarbeitung beginnt am [DATUM] und endet am [DATUM].
Variante
Die Verarbeitung beginnt am [DATUM] und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Haupvertrags durch eine Partei.
Variante
Die Verarbeitung beginnt am [DATUM] und endet nach einmaliger Ausführung.

Vertrag Auftragsverarbeitung personenbezogener Daten

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpas-sung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

3.2 Zweck der Verarbeitung

Die Verarbeitung dient folgendem Zweck: [BESCHREIBUNG]
Variante
Der zugrundeliegende Zweck der Verarbeitung ist in der Leistungsbeschreibung des Hauptvertrages geregelt.

3.3 Art der Daten

Es werden folgende Daten verarbeitet:

- [BESCHREIBUNG] (Bsp: Anrede, Kommunikationsdaten, Vor-und Zuname, Email Adresse, Adresse, Verhaltensdaten)

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- [BESCHREIBUNG] (Bsp: Kunden des Auftraggebers, Interessenten des Auftraggebers, Mitarbeiter des Auftraggebers

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

Hinweis: Es kann sein, dass zusätzlich eine konkrete und nachweisliche Verpflichtung auf bestimmte Geheimhaltungspflichten geboten ist, etwa bei Tätigkeiten für Berufsgeheimnisträger (Insb. im Gesundheitsbereich ist § 203 StGB zu beachten!)

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzan-forderungen laufend angemessen angeleitet und überwacht werden.

Vertrag Auftragsverarbeitung personenbezogener Daten

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.
Variante
Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

(11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

5 Sicherheit der Verarbeitung

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht u-terschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

Vertrag Auftragsverarbeitung personenbezogener Daten

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datembeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

Hinweis: Da dieser Punkt in der Praxis regelmäßig zu Streitigkeiten führt, kann die Verarbeitung in Privatwohnungen auch ausgeschlossen werden. Wird sie zugelassen, sind Kontrollrechte des Auftraggebers aber unverzichtbar.

(7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(8) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Auftraggeber jederzeit auf Verlangen vorzulegen.

Hinweis: Diese Regelung kann zugunsten einer reinen Kontrollberechtigung des Auftraggebers gestrichen werden. Im Ergebnis sollte sie aber sogar im Interesse des Auftragnehmers liegen, da dieser damit in die Lage versetzt wird, seinen Pflichten den ggf. mehreren Kunden gegenüber zu einer Zeit seiner Wahl einheitlich nachzukommen, anstatt übers Jahr verteilt immer wieder unterschiedlichsten Prüfungen ausgesetzt zu sein.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

Vertrag Auftragsverarbeitung personenbezogener Daten

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

Hinweis: Dieser Punkt kann selbstverständlich anders geregelt werden. Dann ist aber entscheidend, dass sämtliche Rechte und Pflichten dieser Vereinbarung mit Wirkung für den Auftraggeber auf Sub-Subunternehmer weiterübertragen werden und der Auftraggeber insbesondere auch direkte Kontrollrechte eingeräumt bekommt.

(6) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist. Soweit aktuell gültige Standardvertragsklauseln auf Basis einer Entscheidung der EU-Kommission (z.B. gemäß Kommissionsentscheidung 2010/87/EU) oder Standarddatenschutzklauseln gem. Art. 46 DSGVO als angemessene Garantien eingesetzt werden, bevollmächtigt der Auftraggeber den Auftragnehmer unter Befreiung vom Verbot der Doppelvertretung gemäß § 181 BGB, zur Vornahme aller hierfür erforderlichen Handlungen sowie zur Abgabe und Entgegennahme von Willenserklärungen gegenüber dem Subunternehmer. Ferner ist der Auftragnehmer berechtigt, die Rechte und Befugnisse des Auftraggebers aus dieser Vereinbarung gegenüber dem Subunternehmer auszuüben.

(9) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen. Der Auftragnehmer bewahrt die Dokumentation über durchgeführte Prüfungen mindestens bis zum Ablauf des dritten Kalenderjahres nach Beendigung der Auftragsverarbeitung auf und legt diese dem Auftraggeber auf Verlangen jederzeit vor.

(10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(11) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(12) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

Vertrag Auftragsverarbeitung personenbezogener Daten

8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutz-pflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeite-ter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. 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;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Vertrag Auftragsverarbeitung personenbezogener Daten

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse XX.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

Vertrag Auftragsverarbeitung personenbezogener Daten

12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftrag-nehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14 Vertragsstrafe

Hinweis: Leider zeigt sich in der Praxis, dass Dienstleister zu häufig die Verpflichtungen aus Auftragsverarbeitungsverträgen nicht ernst nehmen und Versprechungen machen, die nicht eingehalten werden.

(1) Der Auftragnehmer verwirkt bei schuldhaften Verstößen gegen seine Pflichten aus diesem Vertrag eine dem Verstoß angemessene Vertragsstrafe. Die Vertragsstrafe wird insbesondere bei Mängeln in der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen verwirkt. Bei dauerhaften Verstößen gilt jeder Kalendermonat, in dem der Verstoß ganz oder teilweise vorliegt, als Einzelfall. Die Einrede des Fortsetzungszusammenhangs ist ausgeschlossen.

(2) Die Höhe der Vertragsstrafe bestimmt der Auftraggeber nach billigem Ermessen. Entspricht sie nicht der Billigkeit, so wird die Bestimmung durch Urteil getroffen.

(3) Die Vertragsstrafe wird mit Erklärung ihrer Höhe gegenüber dem Auftragnehmer fällig.

(4) Die Vertragsstrafe hat keinen Einfluss auf andere Ansprüche des Auftraggebers.

Vertrag Auftragsverarbeitung personenbezogener Daten

15 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Verein-barung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

16 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum 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.

(3) Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragnehmer

Hinweis: Es handelt sich bei dieser Vereinbarung um einen echten Vertrag, der dementsprechend von einer für das Unternehmen vertretungsbefugten Person zu zeichnen ist. Der Datenschutzbeauftragte ist dies in aller Regel nicht.

Vertrag Auftragsverarbeitung personenbezogener Daten

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informa-tionen.

Die Maßnahmen müssen im Interesse beider Parteien so konkret wie möglich beschrieben werden! Sie sind Maßstab für Kontrollen durch den Auftraggeber und auch für die Frage entscheidend, ob möglicherweise ein Pflichtverstoß vorliegt. In dieser Anlage wird ganz maßgeblich festgelegt, was der Auftragnehmer zu leisten und nachzuweisen hat und was nicht. Unklare oder interpretationsfähige Umschreibungen sind dringend zu vermeiden! Die Angabe der Maßnahmen hat auftragsbezogen zu erfolgen. Die Beschreibung muss aus sich heraus geeignet sein, die Angemessenheit der Maßnahmen zumindest grundsätzlich einzuschätzen und zu beurteilen.

Aufbau / Struktur der Maßnahmen ist grundsätzlich nicht bestimmt. Entscheidend ist der Inhalt. Alternative 1 orientiert sich an den Maßnahmenempfehlungen der ISO 27002 und sorgt für eine klare, detailliertere und überschneidungsfreie Übersicht. Alternative 2 basiert auf einem Vorschlag der Aufsichtsbehörden. Dieser Aufbau nach Gewährleistungszielen ist grober und trennt nicht sauber nach Zielen.

- Organisation der Informationssicherheit
- Personalsicherheit
- Verwaltung der Werte
- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte beim Business Continuity Management
- Compliance

kapit

Vertrag Auftragsverarbeitung personenbezogener Daten

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
- Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)
- Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
  - Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
  - Zugangskontrolle: Keine unbefugte Systembenutzung
  - Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
  - Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
  - Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
  - Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
  - Belastbarkeitskontrolle: Fähigkeit der Systeme, mit risikobedingten Veränderun-gen umzugehen und Aufweisen einer Toleranz und Ausgleichsfähigkeit gegenüber Störungen
- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - Datenschutz-Management: System zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen
  - Incident-Response-Management: System zur Vorbereitung, Identifizierung und Meldung von Sicherheitsvorfällen
  - Datenschutzfreundliche Voreinstellungen:
  - Auftragskontrolle:
  - Datenschutzbeauftragter

Anlage 2 – Zugelassene Subdienstleister

Firma	Anschrift	Auftragsinhalt

Vertrag Auftragsverarbeitung personenbezogener Daten

Anlage 3 – Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung von Weisungen befugt:

Name_____

Kontaktdaten_____

Folgende Personen sind zur Entgegennahme von Weisungen befugt:

Name_____

Kontaktdaten_____

Kontakt zur Meldungen über die Verletzung personenbezogener Daten:

Anlage 4 – Datenschutzbeauftragter

Derzeit ist als interner / externer Datenschutzbeauftragter beim Auftragnehmer bestellt:

Kontaktdaten_____

Angaben zur Fachkunde_____

Bei internen Beauftragten: sonstige Aufgaben im Unternehmen_____

Oder

Beim Auftragnehmer wurde kein Datenschutzbeauftragter bestellt, weil_____