

Mustervertrag für die Auftragsverarbeitung

Die IT-Recht Kanzlei stellt ihren Mandaten den nachstehenden Mustervertrag für eine Auftragsverarbeitung im Sinne des Art. 28 der Datenschutz-Grundverordnung (DSGVO) zur Verfügung, dessen Abschluss erforderlich ist, wenn ein Online-Händler personenbezogene Datenverarbeitungstätigkeiten aus seinem Verantwortungsbereich in seinem Interesse auf einen oder mehrere Dritte überträgt. Mit jedem solcher Dritten, zu denen der Online-Händler in direktem Kontakt steht, ist bei der Auslagerung von Datenverarbeitungsvorgängen der Abschluss eines eigenen Vertrags erforderlich.

Wichtiger Hinweis vorweg

Dieser Mustervertrag ist ein kostenloses und freiwilliges Angebot. Er gehört nicht zum Leistungsumfang Ihrer bei uns gebuchten Schutzpakete. Aus diesem Grund kann die IT-Recht Kanzlei keine Haftung für die Richtigkeit dieses Musters übernehmen und keine individuelle Beratung hinsichtlich des Musters bzw. des daraus erstellten Verarbeitungsverzeichnisses anbieten.

Der nachstehende Mustervertrag ist bewusst händlerfreundlich formuliert, sollte aber trotzdem – um infolge von erforderlichen Abstimmungen mit dem Auftragsverarbeiter anfallenden zeitlichen und organisatorischen Aufwand bestmöglich zu vermeiden – nur verwendet werden, wenn der Auftragsverarbeiter nicht selbst einen entsprechenden Vertrag zur Unterzeichnung bereithält.

Bitte beachten Sie, dass der Mustervertrag nur soweit Mustergültigkeit besitzt, wie generelle Formulierungen und Klauseln möglich sind. Anpassungen und Konkretisierungen durch den Händler sind in jedem Fall erforderlich und betreffen vor allem die Beschreibung der in Auftrag gegebenen Verarbeitungstätigkeit, der Verarbeitungszwecke und der gegenständlichen Daten- und Betroffenenkategorien. Demgegenüber müssen die technischen und organisatorischen Maßnahmen in Anlage 1 vom Auftragsverarbeiter beschrieben werden.

Soweit Ergänzungen erforderlich sind, weist das Muster hierauf durch Eckklammern ([..]) im Fließtext oder durch Textfelder hin.

Nachstehend erfolgt eine nicht abschließende Aufzählung von typischen Verarbeitungskonstellationen im Online-Shop, in denen ein Verarbeitungsvertrag erforderlich (1.) und grundsätzlich nicht erforderlich (2.) ist.

1.) Verarbeitungssituationen, die einen Auftragsverarbeitungsvertrag erfordern

- Die Inanspruchnahme von Webhostern (Strato, Estugo etc.)
- Die Inanspruchnahme einer Shop-Cloud-Lösung oder eines Zahlungs-Hubs (z.B. „Gambio Cloud“ bzw. „Gambio Payment Hub“)
- Die Inanspruchnahme eines IT-Dienstleisters zur Wartung oder Fernwartung
- Die Beauftragung von Software-Entwicklern für Warenwirtschafts-Lösungen
- Die Beauftragung von Newsletter-Versanddienstleistern
- Die Inanspruchnahme von Diensten für automatisierte Kundenbewertungsanfragen durch Bewertungsportale
- Die Inanspruchnahme von Cloud-Hostern
- Der Einsatz von Google Analytics

2.) Verarbeitungssituationen, die keinen Auftragsverarbeitungsvertrag erfordern

- Die Beauftragung von Versanddienstleistern
- Die Weiterleitung von Rechnungen an einen Steuerberater
- Das Anbieten über Verkaufsplattformen wie eBay oder Amazon
- Das Einbinden von Social Plugins
- Die Inanspruchnahme einer Shop-Software auf Installationsbasis (Gambio etc.)

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

und

Online-Händler

Auftragsverarbeiter

Händlerstraße 1

12345 Musterstadt

vertreten durch

vertreten durch

im Folgenden: **Auftraggeber**

im Folgenden: **Auftragnehmer**

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“)

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. 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. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung/Erfassung, Speicherung, Verwendung etc. von [Kategorien der verarbeiteten Daten] von [Kategorien der Betroffenen] zum Zwecke der/des [Angabe des Verarbeitungszwecks]

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag XYZ [Vertragstitel] vom [Datum] (im Folgenden „Hauptvertrag“).

2.2. Die Verarbeitung beginnt am [Datum] und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3. Art und Zweck der Datenverarbeitung

3.1. Der Auftraggeber ist Betreiber eines Online-Shops unter www.xyz.de. Der Auftragnehmer ist ... [geschäftliche Tätigkeit des Auftragnehmers].

3.2. Die Verarbeitung erfolgt in der Art der

[Konkrete Beschreibung der im Auftrag übernommenen Datenverarbeitung unter Beantwortung des folgenden Fragenprogramms:

- Welche konkreten Formen der Datenverarbeitung (Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschung oder Vernichtung) übernimmt der Auftragnehmer für den Auftraggeber?
- Welche personenbezogenen Daten von welchen Betroffenen sind Gegenstand der Verarbeitung?
- Werden diese Daten an den Auftragnehmer vom Auftraggeber übermittelt oder anders mitgeteilt oder erhebt der Auftragnehmer diese originär selbst?]

3.3. Die Verarbeitung dient dem Zweck des/der [konkrete Benennung der Verarbeitungszwecke] für den Auftraggeber und erfolgt aufgrund dessen Interesses an [konkrete Benennung der Interessen des Auftraggebers, die mit der Verarbeitung im Auftrag erfolgt werden, beispielsweise: Rationalisierung, Vereinfachung der Datenorganisation, Entschlackung von Arbeitsabläufen, aber auch: effektives Kundenmanagement, werbliche Ansprache, Marktdurchdringung, Verbesserung der Reichweite]

3.4. Es werden folgende Kategorien personenbezogener Daten verarbeitet:

- Allgemeine Personendaten (Name, Geburtsdatum, Familienstand, Staatsangehörigkeit)
- Kommunikationsdaten (Anschrift, E-Mail-Adresse, Telefonnummer)
- Zahlungsdaten
- Standortdaten (IP-Adresse)
- Gesundheitsdaten

3.5. Von der Verarbeitung betroffen sind:

- Kunden des Auftraggebers
- an den Leistungen des Auftraggebers interessierte Personen
- Besucher der Internetpräsenz des Auftraggebers

4. Pflichten des Auftragnehmers

4.1. 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.

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

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. 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.

4.5. 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 Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. 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.

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

4.9. 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.

4.10. 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 DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) 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.

5.2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten 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.

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

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. 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.

5.6. Die Verarbeitung von Daten im Auftrag in Privatwohnungen sowie die Verarbeitung von Daten im Auftrag mit Privatgeräten sind unter keinen Umständen gestattet.

5.7. 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.

5.8. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihre Wirksamkeit, jederzeit und ohne Vorankündigung zu kontrollieren und zu überprüfen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu diesem Zweck und für die Dauer der Kontrolle Zugang zu allen relevanten Räumlichkeiten sowie Einsicht in und Zugriff auf alle für die Prüfung erforderlichen Dokumente und Systeme zu verschaffen.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

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

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

7. Unterauftragsverhältnisse

7.1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

7.2. 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.

7.3. 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.

7.4. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.5. Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

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

7.7. 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.

7.8. 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 Ziffer 4.10. 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.

7.9. 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.

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

7.11. 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.

7.12. 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.

8. Rechte und Pflichten des Auftraggebers

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

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

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

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen im Sinne der Ziffer 5 sowie ihre Wirksamkeit, 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.

8.5. 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.

9. Mitteilungspflichten

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes 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:

- 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;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- 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

9.2. 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.

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

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

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

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

10.4. 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.

10.5. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

11.1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. 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 X.

11.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

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

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

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

13. Haftung

13.1. 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.

13.2. 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 Auftragnehmer 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.

13.3. 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.

13.4. Die Ziffern 13.2. und 13.3 gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14. Vertragsstrafe

14.1. Bei Verstoß gegen die Bestimmungen dieses Vertrages wird eine verschuldensunabhängige Vertragsstrafe von € X,XX je Einzelfall vereinbart.

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.

14.2. Die Vertragsstrafe lässt andere Ansprüche des Auftraggebers unberührt.

15. Sonderkündigungsrecht

15.1. 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 Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

15.2. 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.

15.3. 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.

15.4. 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 Auftraggeber entstehen.

16. Sonstiges

16.1. 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.

16.2. 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.

16.3. Für Nebenabreden ist die Schriftform erforderlich.

16.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

Unterschriften

.....
Ort, Datum
Auftraggeber

.....
Ort, Datum
Auftragnehmer



Anlage 1

Technische und organisatorische Maßnahmen

Im Folgenden werden die 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 Informationen.



Anlage 2 Zugelassene Subdienstleister

Der Auftraggeber genehmigt der Einsatz der folgenden Subdienstleister durch den Auftragnehmer:



Anlage 3

Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung

2. Weisungsentgegennahme