Auftragsverarbeitung nach Art. 28 DSGVO
Vernichtung von Datenträgern

1. Gegenstand und Dauer der Vereinbarung

Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem vom Auftraggeber erteilten „Auftrag zur Vernichtung von Datenträgern“.

Dauer des Auftrags

Die Dauer dieses Auftrags beginnt ab Unterzeichnung und endet mit Kündigung der Vereinbarung.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

2. Konkretisierung des Auftragsinhalts

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen

Übernahme der Datenträger
Die Abholung erfolgt nach vorheriger Terminvereinbarung. Der zur Übernahme der Datenträger berechtigte Beauftragte des Auftragnehmers übergibt als Berechtigungsnachweis ein vorgefertigtes Übernahmeprotokoll. Name Übergebender und Übernehmender, Fahrzeug-Kennung, Datum, Uhrzeit, Ort, Art, Menge und Verpackung der Datenträger werden bei der Übergabe von den jeweils befugten Mitarbeitern der Vertragspartner auf dem „Auftrag zur Vernichtung von Datenträgern“ bestätigt.

Transport
Der Transport der Datenträger darf nur in geschlossenen Fahrzeugen des Auftragnehmers und/oder Sicherheitsbehältnissen mit eigenem Personal durchgeführt werden. Dabei muss sichergestellt sein, dass keine Datenträger verloren gehen oder entnommen werden können.

Vernichtung
Die übernommenen Datenträger sind in der Regel auf direktem Wege vom Auftragnehmer zu vernichten. Nur in Ausnahmefällen (Kapazitäts- oder Personalengpässe, Ausfall der Vernichtungsanlage) dürfen die Datenträger vorübergehend in abgesperrten Bereichen abgestellt werden. Dabei muss sichergestellt werden, dass Unbefugte keinen Zutritt haben und die Datenträger nicht mit denen anderer Auftraggeber vermischt werden.

Soweit nicht gesondert und ausdrücklich vereinbart, gelten die zu vernichtende Datenträger als der Schutzklasse 2 gemäß DIN 66399-1 zugeordnet. Der Auftragnehmer sichert die Einhaltung der Sicherheitsstufe P4 (Papier), O3 (Optische Datenträger) und T4 (Magnetischem Datenträger) gemäß DIN 66399-2 zu. Der Auftragnehmer ist nicht zur Überprüfung der Schutzklasse oder selbständigen Klassifizierung der übernommenen Datenträger verpflichtet. Die datenschutzkonforme Klassifizierung obliegt dem Auftraggeber. Die Einhaltung einer höheren Sicherheitsstufe ist gesondert zu vereinbaren. Eine Videoüberwachung der Sicherheitszone findet nicht statt.

Der Auftragnehmer hat über die Vernichtung der Datenträger ein Vernichtungsprotokoll abzugeben, die Angaben zu Name Auftragnehmer, Art und Menge der Datenträger, Tag, Uhrzeit, Ort der Vernichtung und Sicherheitsstufe enthält.

Art der personenbezogenen Daten

Gegenstand der Vernichtung personenbezogener Daten entsprechend folgender Datenkategorien:

Abrechnungs-; Planungs-, Vertrags-, Zahlungs- oder Bonitätsdaten; IT Nutzungsdaten (z.B. Log-Daten); Personendaten (Name, Vorname, Geburtsdatum, Straße, PLZ, Ort und eventuell Gesundheits- oder Sozialversicherungsdaten); Kommunikationsdaten (z.B. Telefon-/ Mobilnummer, E-Mail); Bild-, Video oder biometrische Daten usw. (nicht Zutreffendes evtl. streichen)

Kategorien betroffener Personen

Der Kreis der Betroffenen umfasst:

Kunden; Lieferanten; Interessenten; Abonnenten; Beschäftigte; Bewerber; Handelsvertreter; Patienten; Mandanten oder sonst. Ansprechpartner. (nicht Zutreffendes evtl. streichen)

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung des Auftrages erforderlichen technischen und organisatorischen Maßnahmen entsprechend Anlage 1 gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO.

Der Auftragnehmer ermöglicht und unterstützt die Prüfung der Umsetzung der vereinbarten Maßnahmen vor Beginn sowie während der Verarbeitung durch den Auftraggeber.

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Art. 28 Abs. 3 Satz 2 lit.a DS-GVO) folgende Pflichten:

a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artikel 39 DS-GVO ausüben kann. Dessen Kontaktdaten werden im Internet unter http://www.lebenshilfe-ansbach.de/datenschutz/ veröffentlicht.

b) Die Wahrung des Datengeheimnisses entsprechend Art. 28 Abs. 3 Satz 2 lit.b und Art. 29 DS-GVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DS-GVO.

d) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

e) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

f) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, folgende eventuell für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, bspw. Fernmelde-, Bank-, Sozialgeheimnis und Berufsgeheimnisse nach § 203 StGB [anwaltliche/ärztliche/etc.].

g) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

5. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet. Die Zustimmung kann nur erteilt werden,

wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.

Zur Zeit sind für den Auftragnehmer keine Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Nimmt der Auftragnehmer einen Subunternehmer in Anspruch, um Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so wird er diesem Subunternehmer im Wege eines schriftlichen Vertrags dieselben Datenschutzpflichten auferlegen, wie in diesem Vertrag für den Auftragnehmer festgelegt. Dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. die Wartung und Instandhaltung der technischen Anlagen zur Aktenentsorgung, etc.

6. Mitteilungspflichten des Auftragnehmers bei Störungen und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung dieses Vertrages durchführen.

7. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich in Form der Vernichtung der Daten.

a) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

b) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

c) Der Auftraggeber ist berechtigt, sich wie unter Nr. 4 e) festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

e) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

8. Haftung

Der Auftragnehmer haftet nach den gesetzlichen Bestimmungen, sofern der Auftraggeber Schadensersatzansprüche geltend macht, die auf Vorsatz oder grober Fahrlässigkeit, einschließlich Vorsatz oder grober Fahrlässigkeit seiner Vertreter oder Erfüllungsgehilfen, beruhen. Ferner haftet der Auftragnehmer für schuldhafte Verletzungen wesentlicher Vertragspflichten nach den gesetzlichen Bestimmungen. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf. Dies sind insbesondere solche, die den Schutz der verkörperten Daten vor dem Zugriff Unbefugter bis zur Vernichtung sowie die datenschutzkonforme Vernichtung betreffen. Soweit dem Auftragnehmer weder Vorsatz noch grobe Fahrlässigkeit zur Last gelegt werden kann, ist die Schadensersatzhaftung auf den vorhersehbaren, bei Verträgen dieser Art typischerweise eintretenden Schaden begrenzt. Mittelbare Schäden oder Folgeschäden sind nur ersatzfähig, soweit sie typischerweise zu erwarten sind. Eine Änderung der Beweislast zum Nachteil des Vertragspartners ist damit nicht verbunden. Die Haftung wegen schuldhafter Verletzung des Lebens, des Körpers oder der Gesundheit sowie die Haftung nach dem Produkthaftungsgesetz und die Haftung aus Art. 82 DS-GVO bleiben unberührt. Darüberhinausgehende Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen.

Für Ansprüche Dritter gegen den Auftragnehmer aus Art. 82 DS-GVO wird der Gesamtschuldnerinnenausgleich nach Art. 82 Abs. 5 DS-GVO modifiziert in der Form, dass der Auftraggeber zur Freistellung des Auftragnehmers verpflichtet ist, soweit dieser im Außenverhältnis mehr Schadensersatz als gemäß diesem Vertrag vereinbart schuldet.

Im Außenverhältnis haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen nach Art. 82 DS-GVO.

9. Berichtigung, Sperrung und Löschung von Daten und Rückgabe von Datenträgern

Der Auftragnehmer wird nach Übernahme des Datenmaterials vom Auftraggeber dieses Material in Form von Akten oder Datenträgern (z.B. CDs, DVDs etc.) umgehend rückinformationssicher vernichten. Eine andere Form der Datenbearbeitung oder – nutzung erfolgt nicht.

Die im Entsorgungsauftrag vereinbarte Vernichtung des Datenmaterials bestimmt die ursächliche Beauftragung durch den Auftraggeber.

Auf schriftliche Anforderung des Auftraggebers werden noch nicht vernichtete Datenträger auf eigene Kosten zurückgegeben.

Dokumentationen (z.B. Verträge, Vernichtungsbescheinigungen, Rechnungen etc.), die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

10. Sonstiges

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage – Technisch-organisatorische Maßnahmen (TOM)

Anlage – Technisch organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Unbefugten ist der Zutritt zu Datenverarbeitungs- bzw. Datenvernichtungsanlagen zu verwehren.
- Das Betriebsgelände ist nach außen hin eine geschlossene Einheit.
- Das gesamte Betriebsgelände ist eingezäunt.

Zugangskontrolle
Es ist zu verhindern, dass Datenverarbeitungs- bzw. Datenvernichtungsanlagen von Unbefugten genutzt werden können.
- Schlösser an allen Zutrittsmöglichkeiten zur Vernichtungsanlage.
- Anzahl der Mitarbeiter mit Zutrittsberechtigung zur Aktenvernichtung ist minimiert (Schlüsselverzeichnis).
- Während der Öffnungszeiten erfolgt der Zutritt für Betriebsfremde zum Betriebsgelände über den Pförtner (Besucherbuch).
- Festlegung verantwortlicher Personen.

Zugriffskontrolle
Es ist zu gewährleisten, dass die Datenverarbeitungs- bzw. Datenvernichtungsanlagen sowie Transportbehälter ausschließlich von Berechtigten genutzt werden können.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis, TK-, Sozial- und Bankgeheimnis.
- Leiharbeiter werden nicht eingesetzt.
- Öffnen der Transportbehälter bis zur Entleerung in der Aktenvernichtung ist untersagt.

Trennungskontrolle
Es ist zu gewährleisten, dass Entsorgungsmaterial getrennt entsprechend den Anforderungen des Auftraggebers verarbeitet wird.
- Trennung durch verschiedene Behälter.
- Transport für mehrere Auftraggeber in getrennten Behältnissen.
- Vernichtung entsprechend vereinbarter Sicherheitsstufe.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) :
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:
- Nicht auftragsrelevant.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Es ist zu gewährleisten, dass personenbezogene Daten nicht während ihres Transports oder ihrer Lagerung unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Transport des Vernichtungsmaterials ausschließlich in geschlossenen Fahrzeugen.
- Abholung des Aktenmaterials in geschlossenen Behältnissen.
- Transportbegleitschein durch schriftlichen Übernahmeschein.
- Sofern erforderlich - Zwischenlagerung ausschließlich in verschlossener Räumen.

Eingabekontrolle
Es ist zu gewährleisten, dass nachträglich überprüft werden kann, von wem und wann Entsorgungsmaterial der Vernichtung zugeführt wurde.
- Übergabe des Entsorgungsmaterials wird mittels Übergabeschein protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Es ist zu gewährleisten, dass Entsorgungsmaterial gegen zufällige Zerstörung oder Verlust geschützt wird.
- Einsatz von verkehrssicheren Fahrzeugen.
- Brandschutzkonzept.
- Termingetreue Bereitstellung/Abholung der Container.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management
Maßnahmen die gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:
- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit.
- Bestellung eines Datenschutzbeauftragten.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis, TK-, Sozial- und Bankgeheimnis
- Hinreichende Schulung der Mitarbeiter in Datenschutzangelegenheiten.
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO).
- Periodische Prüfung durch Datenschutzbeauftragten.

Incident-Response-Management
Maßnahmen die gewährleisten, dass im Fall von Datenschutzverstößen ein Meldeprozess ausgelöst wird:
- Meldeprozess für Vertrags- und Datenschutzverletzungen gegenüber dem Auftraggeber nach Art. 28 Abs. 3 Satz 3 sowie Art. 33 und Art. 34 DS-GVO).
- Unterstützung für Auftraggeber im Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO) .

Auftragskontrolle
Es ist zu gewährleisten, dass Entsorgungsmaterial nur entsprechend den Weisungen des Auftraggebers vernichtet wird.

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers.
- Prozess zur Erteilung und/oder Befolgung von Weisungen.
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern.
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung.
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis, TK-, Sozial- und Bankgeheimnis.