

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

Zwischen

und

IDS Intelligent Data Systems GmbH
Friedrich der Große 36
44628 Herne

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.
- (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 (DS-GVO) 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 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].

ODER

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

ODER

Die Verarbeitung beginnt am [DATUM] und endet nach einmaliger Ausführung.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art:

- | | |
|---|--|
| <input type="checkbox"/> Erheben und Erfassen | <input type="checkbox"/> Verbreitung oder andere Form der Bereitstellung |
| <input type="checkbox"/> Organisation und Ordnung | <input type="checkbox"/> Löschung oder Vernichtung |
| <input type="checkbox"/> Speicherung | |
| <input type="checkbox"/> Anpassung oder Veränderung | |
| <input type="checkbox"/> Verwendung | |
| <input type="checkbox"/> Auslesen und Abfragen | |
| <input type="checkbox"/> Abgleich oder Verknüpfung | |
| <input type="checkbox"/> Einschränkung | |
| <input type="checkbox"/> Offenlegung durch Übermittlung | |

Die Verarbeitung dient folgendem Zweck: **BESCHREIBUNG**

3.2 Art der Daten und Kategorien betroffener Personen

Es werden folgende personenbezogenen Daten verarbeitet:

- Personenstamm- und Personenverwaltungsdaten (inkl. Arbeitszeiten)
- Bewerberdaten
- Qualifikationsdaten
- Identifikationsdaten
- Kommunikations- und Kontaktdaten (z.B. Telefon, E-Mail)
- Vertragsdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Kundenverhaltensdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Bank- und Kreditkartendaten
- Lohn- und Gehaltsdaten
- Arbeitszeitdaten
- Nutzer- / Protokoll Daten (z.B. An- und Abmeldedaten)
- Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)
- Videodaten
- Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO)
- Sonstige (Erläuterung)

Von der Verarbeitung betroffen sind folgende Personengruppen:

- Beschäftigte
- Auszubildende und Praktikanten
- Bewerber
- Beschäftigte verbundener Unternehmen
- Kunden
- Interessenten (z.B. potenzielle Kunden)
- Lieferanten
- Dienstleister
- Handelsvertreter
- Geschäftspartner
- Ansprechpartner
- Mitglieder
- Abonnenten
- Mieter
- Besucher
- Sonstige (Erläuterung)

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 (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). 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.
- (4) Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden, schriftlich zur Vertraulichkeit verpflichten (gem. Art. 28 Abs. 3 lit. b DS GVO), 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 Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei der Umsetzung der Betroffenenrechte nach Art. 12 bis 23 sowie der Art. 32 bis 36 DS-GVO.
- (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, benennt 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 benannt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit. Einzelheiten zum Datenschutzbeauftragten sind der Anlage 1 zu entnehmen.
- (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 DS-GVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Technische und organisatorische Maßnahmen

- (1) Der Auftragnehmer verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer der Verarbeitung von Auftraggeber-Daten aufrecht zu erhalten, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.
- (2) Die in Anlage 2 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.
- (3) Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (4) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (5) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (6) 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.
- (7) Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind, in Privatwohnungen (Heim-Arbeitsplatz von Beschäftigten des Auftragnehmers; Home-Office) ist nur nach einer vorherigen schriftlichen Zustimmung des Auftraggebers gestattet. Im Ausnahmefall z.B. bei höherer Gewalt kann davon abgewichen werden mit nachträglicher schriftlicher Genehmigung durch den Auftraggeber. Dabei hat der Auftragnehmer sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch am Heim-Arbeitsplatz der Beschäftigten des Auftragnehmers gewährleistet ist. Dazu behält sich der Auftraggeber, unter der angemessenen Berücksichtigung der Persönlichkeitsrechte der Beschäftigten sowie weiterer im jeweiligen Haushalt lebender Personen, die Ausübung des Kontrollrechts vor, ggf. auch anlassbezogen.
- (8) 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.
- (9) 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 auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

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 Unterauftragnehmern (Subunternehmern) ist nur mit schriftlich oder in dokumentiertem elektronischem Format erfolgter Zustimmung des Auftraggebers zugelassen. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden
- (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.
- (3) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (4) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- (5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- (6) 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) 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) 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.
- (8) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig und 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 nach Aufforderung vorzulegen.
- (9) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
- (10) Zurzeit sind die in Anlage 3 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.
- (11) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen wie z.B. Post-, Transport- und Versandleistungen, Wartungs- und Reinigungsleistungen 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

- (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 informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (3) 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.
- (4) 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, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde.
- (5) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
- (6) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen des 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.
- (7) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.
- (8) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.
- (9) Der Auftraggeber vergütet dem Auftragnehmer den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

9 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind anzugeben. Die Mitteilung 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
- (2) Ebenfalls unverzüglich in Schriftform oder dokumentiertem elektronischen Format mitzuteilen sind erhebliche Störungen bei der Auftragserledigung, sicherheitsrelevante Vorfälle und andere Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten sowie Verstöße des Auftragnehmers, der bei ihm beschäftigten Personen oder Dritte gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden sowie anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 der DS-GVO im erforderlichen Umfang zu unterstützen.

10 Weisungen

- (1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Dieser erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in schriftlicher oder elektronischer Form zu dokumentieren. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens Textform). Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
- (2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 4.
- (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) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung aufzubewahren.

11 Beendigung des Auftrags

- (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 löschen bzw. zu vernichten oder an den Auftraggeber zu übergeben. Dies gilt entsprechend für sämtliche vorhandenen 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.
- (2) Der Auftragnehmer ist verpflichtet, die unverzügliche Löschung bzw. Vernichtung oder 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 den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Vergütung

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

13 Haftung und Recht auf Schadenersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

14 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 Vereinbarung 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.

15 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) Sollten Daten bzw. Datenträger 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 informieren. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten bzw. Datenträger ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.
- (3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB durch den Auftragnehmer 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.

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

ANLAGE 1 zum Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Datenschutzbeauftragter

Derzeit ist als interner / externer Datenschutzbeauftragter beim Auftragnehmer benannt:

Kontaktdaten

Bei internen Beauftragten: sonstige Aufgaben im Unternehmen

Oder

Beim Auftragnehmer wurde kein Datenschutzbeauftragter benannt, weil...

ANLAGE 2 zum Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Technisch-organisatorische Maßnahmen des Auftragnehmers

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

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- 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;
- Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Personenbezogene Daten sind abhängig von der Kritikalität verschlüsselt zu übertragen und zu speichern. Im Zweifel muss von einer hohen Kritikalität ausgegangen werden.

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

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement;

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

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. Backup-Strategie (online/offline; onsite/offsite), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche 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, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management, u.a. Vorfalleaktionsplan, Angriffserkennung, Monitoring und Alarmierung;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.

ANLAGE 3 zum Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Unterauftragsverhältnisse (Subunternehmer)

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Unternehmen und Anschrift	Art und Zweck der Verarbeitung	Art der Daten	Betroffenenkategorien

ANLAGE 4 zum Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Derzeit fungieren auf Seiten des Auftraggebers folgende Personen als **Weisungsberechtigte**:

Weisungsberechtigte (Vorname, Name, Organisationseinheit, Telefon):



Die Parteien vereinbaren als **Empfangsberechtigte** für Weisungen auf Seiten des Auftragnehmers folgende Personen:

Empfangsberechtigte (Vorname, Name, Organisationseinheit, Telefon):

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.