Vertrag zur Verarbeitung von Daten im Auftrag

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen

siehe Angaben zum Auftraggeber (nachfolgend „Auftraggeber“)

und

dilohver GmbH, Hochstr. 21-23, 82024 Taufkirchen (nachfolgend „Auftragnehmer“)

(Auftraggeber und Auftragnehmer gemeinsam nachfolgend: „die Parteien“)

Ziel dieses Vertrags

Mit diesem Auftragsverarbeitungsvertrag regeln die Parteien ihre datenschutzrechtlichen Rechte und Pflichten, soweit der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Der Vertrag konkretisiert die Anforderungen des Art. 28 DSGVO und ergänzt die zwischen den Parteien bestehenden Hauptverträge für die jeweils beauftragten Verarbeitungsleistungen.

Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder von ihm eingesetzte Personen personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO, soweit sich aus dem jeweiligen Hauptvertrag oder zwingendem Recht nichts anderes ergibt.

PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

1.1 Gegenstand dieses Auftragsverarbeitungsvertrags ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in Anlage 1. Soweit dies für die konkret beauftragte Leistung erforderlich ist, kann die Verarbeitung auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO umfassen, insbesondere Gesundheitsdaten sowie Angaben, aus denen sich gegebenenfalls eine religiöse Zugehörigkeit ableiten lässt.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung findet grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums statt, sofern sich aus den Anlagen nichts anderes ergibt. Eine Verarbeitung in einem Drittland oder eine Übermittlung an einen Empfänger in einem Drittland ist zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Für den Einsatz von Unterauftragnehmern gelten ergänzend die Regelungen in Ziffer 11.

3. LAUFZEIT

3.1 Dieser Vertrag gilt für die Dauer sämtlicher Hauptverträge, in deren Rahmen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Eine gesonderte ordentliche Kündigung dieses Vertrags wird erst wirksam, sobald keine hiervon erfasste Verarbeitungsleistung mehr besteht. Die Pflichten, die ihrem Zweck nach über die Beendigung hinauswirken, bleiben unberührt.

3.2 Der Auftraggeber kann die betroffene Verarbeitungsleistung aus wichtigem Grund außerordentlich kündigen, wenn der Auftragnehmer schwerwiegend gegen zwingende Datenschutzvorschriften oder wesentliche Pflichten dieses Vertrags verstößt und der Verstoß nicht innerhalb einer angemessenen Abhilfefrist beseitigt wird. Einer Abhilfefrist bedarf es nicht, wenn sie gesetzlich unzulässig oder wegen Art und Schwere des Verstoßes unzumutbar ist.

3.3 Der Auftragnehmer ist berechtigt, die betroffene Verarbeitung auszusetzen und nach erfolgloser angemessener Abhilfefrist außerordentlich zu kündigen, wenn der Auftraggeber trotz Hinweises an einer rechtswidrigen Weisung festhält, die erforderliche Rechtmäßigkeit der Verarbeitung nicht sicherstellt oder sonstige wesentliche datenschutzrechtliche Pflichten verletzt. Zwingende gesetzliche Pflichten des Auftragnehmers bleiben unberührt.

4. WEISUNG

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4.2 Weisungen, die Gegenstand, Art, Zweck oder Umfang der in Anlage 1 beschriebenen Verarbeitung wesentlich ändern oder erweitern, bedürfen einer entsprechenden Vereinbarung in schriftlicher oder elektronischer Form. Weisungen außerhalb des im Hauptvertrag vereinbarten Leistungsumfangs können, soweit rechtlich zulässig, als zusätzliche Leistung nach den jeweils vereinbarten Vergütungssätzen abgerechnet werden.

4.3 Weisungen des Auftraggebers sind in Textform zu erteilen oder vom Auftragnehmer entsprechend zu dokumentieren. Die Parteien bewahren die Weisungsdokumentation für die Dauer der Verarbeitung und anschließend so lange auf, wie dies zur Erfüllung gesetzlicher Nachweis- oder Aufbewahrungspflichten erforderlich ist.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine Weisung seiner Auffassung nach gegen die DSGVO oder andere einschlägige Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis sie geändert oder zurückgenommen wurde oder ihre Rechtmäßigkeit nachvollziehbar nachgewiesen ist. Eine bloße Bestätigung einer fortbestehend rechtswidrigen Weisung verpflichtet den Auftragnehmer nicht zu deren Ausführung. Weitergehende Rechte nach Ziffer 3.3 bleiben unberührt.

4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. PFLICHTEN DES AUFTRAGGEBERS UND UNTERSTÜTZUNG DURCH DEN AUFTRAGNEHMER

5.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen der erforderlichen Rechtsgrundlagen nach Art. 6 und, soweit einschlägig, Art. 9 DSGVO, für die Erfüllung der Informationspflichten sowie für die Wahrung der Betroffenenrechte verantwortlich. Er stellt sicher, dass die Beauftragung und die von ihm erteilten Weisungen datenschutzrechtlich zulässig sind.

5.2 Der Auftraggeber trägt dafür Sorge, dass die dem Auftragnehmer bereitgestellten personenbezogenen Daten für die beauftragte Verarbeitung erforderlich, im Rahmen seines Verantwortungsbereichs richtig und vollständig sowie rechtmäßig erhoben sind. Fehlerhafte, unvollständige oder geänderte Angaben teilt er dem Auftragnehmer unverzüglich mit.

5.3 Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter und angemessenen erforderlichen Aufwendungen frei, soweit diese auf einer vom Auftraggeber zu vertretenden Verletzung seiner datenschutzrechtlichen Pflichten, einer rechtswidrigen Weisung oder einer von ihm zu vertretenden unzulässigen Bereitstellung personenbezogener Daten beruhen. Dies gilt nicht, soweit der Auftragnehmer den anspruchsbegründenden Umstand selbst zu vertreten hat.

5.4 Der Auftragnehmer ergreift unter Berücksichtigung der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Art. 12 bis 22 DSGVO angemessen zu unterstützen.

5.5 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber angemessen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und gegebenenfalls bei der vorherigen Konsultation der zuständigen Aufsichtsbehörde.

5.6 Wendet sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde unmittelbar an den Auftragnehmer, soweit die unter diesem Vertrag verarbeiteten personenbezogenen Daten betroffen sind, informiert der Auftragnehmer den Auftraggeber unverzüglich, sofern dem keine gesetzliche Verpflichtung entgegensteht. Der Auftragnehmer beantwortet Betroffenenanfragen grundsätzlich nicht eigenständig, soweit er hierzu nicht gesetzlich verpflichtet oder vom Auftraggeber angewiesen ist.

5.7 Unterstützungsleistungen, die über den im Hauptvertrag vereinbarten oder nach Art. 28 DSGVO üblichen Mitwirkungsumfang hinausgehen, kann der Auftragnehmer nach angemessenem tatsächlichem Aufwand und den jeweils vereinbarten Vergütungssätzen abrechnen, sofern der zusätzliche Aufwand nicht durch einen vom Auftragnehmer zu vertretenden Datenschutzverstoß verursacht wurde. Gesetzlich zwingende Mitwirkungspflichten bleiben unberührt.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die nach Art. 28 DSGVO erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung. Der Nachweis kann insbesondere durch die Bereitstellung der vereinbarten technischen und organisatorischen Maßnahmen, geeigneter Dokumentationen, Prüfberichte, Zertifikate oder sonstiger belastbarer Nachweise erfolgen.

6.2 Der Auftraggeber ist berechtigt, die Einhaltung der Pflichten aus diesem Vertrag selbst oder durch einen zur Vertraulichkeit verpflichteten unabhängigen Prüfer zu kontrollieren. Soweit kein konkreter Anlass, keine behördliche Anforderung oder keine sonstige besondere gesetzliche Notwendigkeit besteht, sind Vor-Ort-Prüfungen grundsätzlich mit mindestens zehn Werktagen Vorlauf anzukündigen, während der üblichen Geschäftszeiten durchzuführen und auf ein angemessenes Maß zu beschränken. Routineprüfungen sollen grundsätzlich nicht häufiger als einmal pro Kalenderjahr erfolgen.

6.3 Vor einer Vor-Ort-Prüfung sollen zunächst die vom Auftragnehmer bereitgestellten Nachweise ausgeschöpft werden, soweit diese zur Prüfung ausreichen. Kontrollen dürfen den Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen und weder personenbezogene Daten anderer Auftraggeber noch Geschäfts- und Betriebsgeheimnisse oder sicherheitskritische Informationen offenlegen, soweit dies für den Prüfzweck nicht erforderlich ist. Ein Prüfer darf kein unmittelbarer Wettbewerber des Auftragnehmers sein, sofern der Auftraggeber keinen gleichwertigen Schutz der berechtigten Interessen des Auftragnehmers sicherstellt.

6.4 Jede Partei trägt ihre eigenen Kosten der Prüfung. Soweit der Auftragnehmer bei einer Routineprüfung Unterstützungsleistungen erbringt, die den gesetzlich geschuldeten üblichen Aufwand wesentlich überschreiten, kann er den zusätzlichen Aufwand nach den vereinbarten Vergütungssätzen abrechnen. Dies gilt nicht, soweit die Prüfung einen wesentlichen vom Auftragnehmer zu vertretenden Verstoß bestätigt.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Auftragnehmer hat einen Datenschutzbeauftragten nach den Vorgaben der Datenschutz-Grundverordnung (DSGVO) bestellt. Die Kontaktdaten erhält der Auftraggeber auf Anfrage per E-Mail. Etwaige Datenschutzanfragen können an datenschutz@dilohver.de gestellt werden.

8. VERTRAULICHKEIT

8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (ANLAGE 2)

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive

Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.

9.2 Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in Anlage 2 beschrieben.

9.3 Der Auftragnehmer kann die technischen und organisatorischen Maßnahmen im Rahmen der technischen und organisatorischen Weiterentwicklung anpassen, sofern das für die konkrete Verarbeitung erforderliche Schutzniveau insgesamt nicht wesentlich unterschritten wird. Wesentliche Änderungen werden dokumentiert; zwingende Anforderungen nach Art. 32 DSGVO bleiben unberührt.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt geworden ist, soweit hiervon im Auftrag verarbeitete personenbezogene Daten betroffen sind. Die Mitteilung enthält, soweit dem Auftragnehmer zu diesem Zeitpunkt bekannt und verfügbar, die Informationen, die der Auftraggeber zur Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO benötigt; fehlende Informationen können ohne unangemessene Verzögerung nachgereicht werden.

10.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen angemessen bei der Untersuchung, Eindämmung und Behebung einer solchen Verletzung sowie bei den hieraus folgenden gesetzlichen Melde- und Benachrichtigungspflichten.

10.3 Sollten die personenbezogenen Daten, die unter dieser Vereinbarung verarbeitet werden beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit eine Datenschutzaufsichtsbehörde den Auftragnehmer prüft, informiert der Auftragnehmer den Auftraggeber über für die vertragsgegenständliche Verarbeitung relevante Ergebnisse, soweit dies rechtlich zulässig und zur Erfüllung der Pflichten des Auftraggebers erforderlich ist. Festgestellte, für die Auftragsverarbeitung relevante Mängel behebt der Auftragnehmer innerhalb einer unter Berücksichtigung des Risikos und etwaiger behördlicher Vorgaben angemessenen Frist.

10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

11.1 Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragnehmer sowie zum künftigen Hinzuziehen oder Ersetzen weiterer Unterauftragnehmer im Sinne des Art. 28 Abs. 2 DSGVO. Die in Anlage 3 beschriebenen Verarbeitungen gelten jeweils nur, soweit der betreffende Unterauftragnehmer für die konkret beauftragte Leistung tatsächlich eingesetzt wird; die Auflistung erweitert weder Gegenstand noch Zweck der Hauptleistung.

11.2 Der Auftragnehmer informiert den Auftraggeber über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers grundsätzlich mindestens 14 Kalendertage vor dessen Einsatz in Textform. Der Auftraggeber kann innerhalb dieser Frist aus objektiv nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Können die Parteien einen berechtigten Widerspruch nicht angemessen lösen, kann der Auftragnehmer auf den Einsatz für die betroffene Leistung verzichten, eine zumutbare Alternative anbieten oder die betroffene Verarbeitungsleistung mit angemessener Frist beenden; das gleiche Recht steht dem Auftraggeber für die betroffene Verarbeitungsleistung zu.

11.3 Der Auftragnehmer stellt durch einen Vertrag in schriftlicher oder elektronischer Form sicher, dass dem Unterauftragnehmer im Wesentlichen dieselben Datenschutzpflichten auferlegt werden, die dem Auftragnehmer nach diesem Vertrag und Art. 28 Abs. 3 DSGVO obliegen.

11.4 Soweit ein Unterauftragnehmer personenbezogene Daten in einem Drittland verarbeitet oder ein Drittlandtransfer stattfindet, stellt der Auftragnehmer sicher, dass zusätzlich die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.5 Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, bleibt der Auftragnehmer dem Auftraggeber gegenüber nach Maßgabe des Art. 28 Abs. 4 DSGVO für die Einhaltung der Pflichten des Unterauftragnehmers verantwortlich. Unmittelbare Weisungs- oder Kontrollrechte des Auftraggebers gegenüber einem Unterauftragnehmer bestehen nur, soweit dies gesetzlich erforderlich oder im Einzelfall ausdrücklich vereinbart ist.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

12.1 Nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen gibt der Auftragnehmer nach Wahl des Auftraggebers die im Auftrag verarbeiteten personenbezogenen Daten zurück oder löscht sie, einschließlich vorhandener Kopien, soweit nicht eine gesetzliche Verpflichtung zur weiteren Speicherung besteht. Soweit eine gesetzliche Aufbewahrungspflicht besteht, wird die Verarbeitung für die Dauer der Aufbewahrung auf die gesetzlich zulässigen Zwecke beschränkt; die Pflichten zur Sicherheit der Verarbeitung gelten fort.

12.2 Die Löschung aus Produktivsystemen erfolgt innerhalb einer angemessenen, technisch und organisatorisch erforderlichen Frist nach dem Stand der Technik. Personenbezogene Daten in Sicherungskopien werden im Rahmen der festgelegten Backup- und Überschreibzyklen gelöscht, sofern eine selektive vorzeitige Löschung technisch nicht ohne unverhältnismäßigen Aufwand möglich ist. Bis zur endgültigen Löschung bleiben diese Daten gesperrt beziehungsweise auf Wiederherstellungszwecke beschränkt und dürfen nicht anderweitig verarbeitet werden.

12.3 Der Auftragnehmer dokumentiert die ordnungsgemäße Rückgabe beziehungsweise Löschung in angemessener Weise und stellt dem Auftraggeber auf Verlangen innerhalb angemessener Frist eine entsprechende Bestätigung zur Verfügung. Gesetzlich erforderliche Nachweise und Protokolle dürfen im erforderlichen Umfang aufbewahrt werden.

13. HAFTUNG

13.1 Die zwingende gesetzliche Haftung gegenüber betroffenen Personen, insbesondere nach Art. 82 DSGVO, bleibt unberührt. Der Auftragnehmer haftet danach insbesondere für Schäden, soweit er gegen speziell an Auftragsverarbeiter gerichtete Pflichten der DSGVO verstößt oder rechtmäßige Weisungen des Auftraggebers nicht beachtet beziehungsweise außerhalb dieser Weisungen handelt.

13.2 Im Innenverhältnis der Parteien gelten, soweit gesetzlich zulässig, die im jeweiligen Hauptvertrag vereinbarten Haftungsbeschränkungen auch für Ansprüche aus diesem Auftragsverarbeitungsvertrag. Zwingende gesetzliche Ausgleichs- und Regressansprüche, insbesondere nach Art. 82 Abs. 5 DSGVO, bleiben unberührt; die Parteien tragen Schäden im Innenverhältnis entsprechend ihrem jeweiligen Verantwortungsanteil.

13.3 Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter und angemessenen erforderlichen Aufwendungen frei, soweit diese auf einer vom Auftraggeber zu vertretenden rechtswidrigen Weisung, fehlenden Rechtsgrundlage, Verletzung eigener Informations- oder Betroffenenpflichten oder sonstigen vom Auftraggeber zu vertretenden Datenschutzverletzung beruhen. Die Freistellung gilt nicht, soweit der Auftragnehmer den betreffenden Umstand selbst zu vertreten hat.

14. SCHLUSSBESTIMMUNGEN

14.1 Gesetzlich oder nach diesem Vertrag geschuldete Herausgabe- und Löschpflichten personenbezogener Daten darf der Auftragnehmer nicht allein wegen offener Vergütungsansprüche verweigern. Im Übrigen bleiben gesetzliche Zurückbehaltungsrechte und Sicherungsrechte des Auftragnehmers unberührt, soweit deren Ausübung mit den datenschutzrechtlichen Pflichten vereinbar ist.

14.2 Änderungen und Ergänzungen dieses Vertrags bedürfen einer schriftlichen oder elektronischen Form im Sinne des Art. 28 Abs. 9 DSGVO. Dies gilt auch für eine Änderung dieses Formerfordernisses, soweit nicht zwingendes Recht entgegensteht.

14.3 Sollte eine Bestimmung dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Soweit datenschutzrechtliche Regelungen dieses Vertrags mit Regelungen eines Hauptvertrags kollidieren, gehen für die Auftragsverarbeitung die Bestimmungen dieses Vertrags vor; im Übrigen bleibt der Hauptvertrag unberührt.

_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlagen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Weitere Auftragsverarbeiter

Anlagen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Weitere Auftragsverarbeiter

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Erbringung der beauftragten Dienstleistung gemäß Auftragsformular des Auftragnehmers, i.d.R. Durchführung der Lohn- und Gehaltsabrechnung sowie Tätigkeiten im direkten oder indirekten Zusammenhang mit dem Lohnsteuerabzug und der Lohnbuchführung. Erfüllung von vertraglichen Verpflichtungen und gesetzlichen Anforderungen.
Art und Umfang der Datenverarbeitung–	Automatisierte Verarbeitung: Alle Daten werden elektronisch erfasst, gespeichert und verarbeitet. Dies umfasst den Einsatz von Software für Lohn- und Gehaltsabrechnungen, die Datenbankverwaltung und den sicheren Austausch mit Dritten für die elektronische Übermittlung von Meldungen an Behörden, wie z.B. die Sozialversicherungsbehörden und das Finanzamt.
Art der Daten	**Mitarbeiterstammdaten:** Name Anschrift Geburtsdatum Sozialversicherungsnummer Steueridentifikationsnummer Bankverbindung **Beschäftigungsdaten:** Anstellungsdatum Stellenbezeichnung Arbeitszeitmodell (Vollzeit, Teilzeit, Minijob, kurzfristig Beschäftigter, Praktikant) Tarifvertragliche Zugehörigkeit **Lohn- und Gehaltsdaten:** Bruttogehalt Zuschläge (z.B. Überstunden, Nachtarbeit) Abzüge (Steuern, Sozialversicherungsbeiträge) Nettogehalt **Urlaubs- und Fehlzeiten:** Urlaubsansprüche Krankheitszeiten Sonstige Fehlzeiten (z.B. Elternzeit) **Sonstige relevante Informationen:** Betriebliche Altersvorsorge Bonus- und Prämienzahlungen Fortbildungsmaßnahmen
Kategorien betroffener Personen	Alle Angestellten des Auftraggebers, sowie ehemalige Mitarbeiter, die für Abrechnungen oder Nachfragen benötigt werden.

Anlage 2: Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOM) sind zentral für die Datenschutzpraxis. Sie beschreiben Maßnahmen, die in erster Linie zum Schutz der verarbeiteten Daten ergriffen werden. Unterschieden werden technische Maßnahmen, die physisch umsetzbar sind, von organisatorischen Maßnahmen, die Verfahren, Abläufe und Handlungsanweisungen betreffen. Für diese TOM definiert das Standard-Datenschutz-Modell der deutschen Aufsichtsbehörden sieben Gewährleistungsziele. Die Checkliste zeigt übersichtlich eine Auswahl von Maßnahmen nach dem Standard-Datenschutz-Modell (SDM) auf:

• Maßnahmen zur Datenminimierung, wie z. B. die Implementierung von Sperr- und Löschroutinen

• Maßnahmen zur Transparenz, wie z. B. die Protokollierung von Zugriffen und Änderungen

• Maßnahmen zur Intervenierbarkeit, wie z. B. die Einrichtung einer Deaktivierungsmöglichkeit für einzelne Funktionalitäten

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Besucher in Begleitung
Sicherheitsschlösser	Sorgfalt bei Auswahl Reinigungsdienst
	Clean-Desk-Policy
	Grundsätzlich digitale Verarbeitung; unvermeidbar anfallende Papierunterlagen werden nach Wegfall des Verarbeitungszwecks sicher nach DIN 66399 vernichtet.

1.2 Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
2-Faktor-Identififiezierung	Erstellen von Benutzerprofilen
2 Fach Login mit unterschiedlichem Passwort zum Zugang auf unseren Server	Zentrale Passwortvergabe
Anti-Viren-Software Laptops	Richtlinie „Sicheres Passwort“
Anti-Viren-Software Geschäftshandys	Richtlinie „Sicheres Passwort“
Firewall	Richtlinie „Löschen / Vernichten“
Mobile Device Management	Richtlinie „Clean- Desk“
Einsatz VPN bei Remote-Zugriffen	Allg. Richtlinie Datenschutz und / oder Sicherheit
Verschlüsselung von Datenträgern	Mobile Device Policy
Verschlüsselung Smartphones	Anleitung „Manuelle Desktopsperre“
Gehäuseverriegelung	
BIOS Schutz (separates Passwort)	
Sperre externer Schnittstellen (USB)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	

1.3 Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte
Externe Aktenvernichtung nach DIN 66399 entsprechend dem jeweiligen Schutzbedarf	Minimale Anzahl an Administratoren
Physische Löschung von Datenträgern	Datenschutztresor
	Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Festlegung von Datenbankrechten
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

2.0 Integrität
2.1 Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Verschlüsselung	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Einsatz von VPN	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
Bereitstellung über verschlüsselte Verbindungen wie z.B.: sftp, https	

2.2 Eingangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen

3.0 Verfügbarkeit und Belastbarkeit
3.1 Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Mit Sorgfalt ausgewählter externer Server sowie regelmäßige Tests zur Datenwiederherstellung Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

4.0 Verfügbarkeit und Belastbarkeit
4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich

4.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind.	
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

Anlage 3: Weitere Auftragsverarbeiter

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
Agenda Informationssysteme GmbH & Co. KG Oberaustraße 14 83026 Rosenheim	**Erfassung von Personaldaten:** Die Software verarbeitet personenbezogene Daten von Mitarbeitern, wie Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern, Steueridentifikationsnummern und Bankverbindungen. **Erfassung von Arbeitszeitdaten:** Die Software kann Arbeitszeitdaten, Überstunden, Urlaubs- und Krankheitszeiten sowie Abwesenheiten verarbeiten. **Berechnung von Löhnen und Gehältern:** Die Software führt Berechnungen durch, um Brutto- und Nettolöhne zu ermitteln, einschließlich der Abzüge für Steuern, Sozialversicherungsbeiträge und andere Abgaben. **Erstellung von Abrechnungen:** Die Software generiert Lohn- und Gehaltsabrechnungen für die Mitarbeiter, die die berechneten Beträge und Abzüge ausweisen. **Übermittlung von Daten:** Die Software kann Daten an Finanzämter, Sozialversicherungsträger und andere relevante Stellen übermitteln. **Archivierung:** Die Software speichert historische Lohn- und Gehaltsdaten für zukünftige Referenzen, Audits oder rechtliche Anforderungen. **Reporting:** Die Software kann Berichte erstellen, die Informationen über Lohnkosten, Personalaufwand und andere relevante Kennzahlen liefern.	**Berechnung von Löhnen und Gehältern:** Die Software ermöglicht die automatisierte Berechnung von Brutto- und Nettolöhnen unter Berücksichtigung von Steuern, Sozialversicherungsbeiträgen und weiteren Abzügen. **Erstellung von Abrechnungen:** Die Software generiert Lohn- und Gehaltsabrechnungen für die Mitarbeiter, die die einzelnen Positionen und Abzüge klar auflisten. **Dokumentation und Archivierung:** Die Software sorgt für die ordnungsgemäße Dokumentation und Archivierung der Lohnabrechnungen und relevanten Daten, um gesetzlichen Anforderungen zu genügen. **Meldungen an Behörden:** Die Software kann die Erstellung von Meldungen an Finanzbehörden, Sozialversicherungsträger und andere relevante Institutionen unterstützen. **Datenmanagement:** Verwaltung von Mitarbeiterdaten, einschließlich persönlicher Informationen, Beschäftigungsdaten und Bank-verbindungen, die für die Lohnabrechnung erforderlich sind.	**Personen-stammdaten:** 1) Vorname und Nachname 2) Geburtsdatum 3) Adresse 4) Telefonnummer 5) E-Mail-Adresse **Beschäftigungs-daten:** 1) Personalnummer 2) Beschäftigungs-beginn und ende 3) Position/Titel **Vergütungsdaten:** 1) Brutto- und Nettogehalt 2) Zuschläge, z.B. Überstunden, Weihnachtsgeld 3) Abzüge, z.B. Steuern, Sozial-versicherungsbeiträge **Bankdaten:** 1) Kontoinformationen für die Gehalts-überweisung **Urlaubs- und Fehlzeiten:** 1) Urlaubsansprüche 2) Krankheitstage 3) sonstige Abwesenheiten **Steuerdaten:** 1) Steuer-Identifikations-nummer 2) Steuerklasse **Sozialversicherungs-daten** 1) Sozial-versicherungs-nummer 2) Informationen zur Kranken- und Rentenversicherung	**Identifikationsdaten:** Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Adresse. **Beschäftigungsdaten:** Personalnummer, Beschäftigungsart, Eintrittsdatum, Austrittsdatum, Abteilung, Position. **Vergütungsdaten:** Bruttogehalt, Nettogehalt, Zuschläge, Abzüge, Sozialversicherungsbeiträge. **Zeiterfassungsdaten:** Arbeitszeiten, Überstunden, Fehlzeiten, Urlaubsansprüche. **Bankverbindungsdaten:** Kontoinhaber, IBAN, BIC für die Gehaltsüberweisung. **Steuerdaten:** Steueridentifikationsnummer, Steuerklasse, Kirchensteuerpflicht. **Sozialversicherungsdaten:** Sozialversicherungsnummer, Angaben zur Krankenversicherung, Rentenversicherung.

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
IP-Projects GmbH & Co. KG Am Vogelherd 14 97295 Waldbrunn	**Hosting und Betrieb von IT-Infrastruktur** Bereitstellung und Betrieb technischer Server- und Speichersysteme zur Verarbeitung der im Rahmen der beauftragten Dienstleistungen anfallenden Daten. **Datenübertragung** Bereitstellung verschlüsselter Datenübertragungswege und -tools für den sicheren Austausch von Dateien und Informationen. **E-Mail-Dienste** Bereitstellung und Betrieb der E-Mail-Infrastruktur für den Versand, Empfang und die Speicherung dienstlicher E-Mail-Kommunikation.	**Technische Bereitstellung und Absicherung** Technische Bereitstellung und Absicherung der vom Auftragnehmer zur Erbringung der beauftragten Dienstleistungen eingesetzten IT-, Kommunikations- und Datenübertragungsinfrastruktur. **Speicherung und Sicherung** Sichere Speicherung, Datensicherung, Wiederherstellung und technische Administration der Systeme. **Kommunikation und Datenaustausch** Sichere Übermittlung und Verarbeitung von E-Mail-Kommunikation sowie Dateien und Daten zwischen Auftragnehmer, Auftraggeber und berechtigten Stellen.	**Mitarbeiterstammdaten und Beschäftigungsdaten** Lohn- und Gehaltsdaten Sozialversicherungs- und Steuerdaten Bankverbindungsdaten Kommunikations- und Kontaktdaten Dokumente und Dateien, die im Rahmen der beauftragten Dienstleistung übermittelt oder gespeichert werden Technische Protokoll-, Zugriffs- und Verbindungsdaten jeweils nur, soweit diese über die bereitgestellte Infrastruktur verarbeitet werden.	Beschäftigte und ehemalige Beschäftigte des Auftraggebers Ansprechpartner und Beschäftigte des Auftraggebers Kommunikationspartner des Auftraggebers und des Auftragnehmers Sonstige Personen, deren personenbezogene Daten im Rahmen der beauftragten Dienstleistung über die bereitgestellte Infrastruktur verarbeitet werden