



AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 DSGVO

zwischen dem Verantwortlichen

.....
– nachfolgend „Auftraggeber“ genannt –

und dem Auftragsverarbeiter

Bewachungsdienst Dipl.-Kfm. Helmut Ehrl GmbH
Ringbergstr. 1
81673 München

– nachfolgend „Auftragnehmer“ genannt –
– nachfolgend zusammen „Parteien“ genannt –



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 der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts anderes ergibt. Vor Verlagerung der Verarbeitung in ein Drittland informiert der Auftragnehmer den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. LAUFZEIT

- 3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei analog zu den Vertragsbedingungen des Hauptvertrages gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrags bis zu der regulären Beendigung des Hauptvertrags/ der Hauptverträge fort.
- 3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die

Bestimmungen dieses Vertrags vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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 Falls Weisungen, die unter Ziffer 1 der Anlage dieses Vertrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.
- 4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrags und anschließend noch für drei Jahre aufzubewahren.
- 4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

- 5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur

Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

- 5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.
- 5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.
- 5.4 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers (Gesetzes- oder Vertragsverstoß) zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

- 6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.
- 6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei. Soweit nicht aus vom Auftraggeber zu dokumentierenden dringlichen Gründen (z.B. einem Verstoß gegen die in diesem Vertrag festgelegten Pflichten) anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt.
- 6.3 Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen.

- 6.4 Der Auftraggeber vergütet dem Auftragnehmer den angemessenen Aufwand, der ihm im Rahmen der Kontrolle entsteht. Etwaige Vergütungsansprüche seitens des Auftragnehmers bestehen nicht, wenn die Kontrollen aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich sind.
- 6.5 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltung der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrags unter Ziffer 2 angeführt, soweit für den Auftragnehmer ein Datenschutzbeauftragter bestellt sein muss oder freiwillig bestellt ist.

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

- 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 in Ziffer 4 der Anlage festgelegten technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.
- 9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 4 vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind in schriftlicher Form oder einem elektronischen Format zu vereinbaren.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMER UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

- 10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.
- 10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.
- 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 Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht festgestellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.
- 10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

- 11.1 Vor der eventuellen Hinzuziehung oder Ersetzung von Unterauftragnehmern informiert der Auftragnehmer den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
- 11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.
- 11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- 11.4 Zum Zeitpunkt dieser Vereinbarung setzt der Auftragnehmer keine Unterauftragsverarbeiter ein. Sollte dies unter Einhaltung der Voraussetzungen aus Ziffer 11 dieses Vertrages zukünftig der Fall sein, können diese in Ziffer 3 der Anlage ergänzt werden.
- 11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unterauftragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

- 12.1 Der Auftragnehmer ist nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.
- 12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 12.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13. HAFTUNG

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

14. SCHLUSSBESTIMMUNGEN

-
- 14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.
- 14.2 Die Anlage oder im Falle mehrerer abgeschlossener Hauptverträge die Anlagen zu diesem Vertrag sind wesentlicher Bestandteil desselben.
- 14.3 Für Änderungen oder Nebenabreden ist die Schriftform erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.



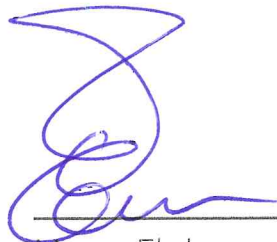
- 14.4 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.

Für den Auftraggeber:

Ort, Datum

Für den Auftragnehmer:

München, 06.05.2025
Ort, Datum


Marco Ehrl
Geschäftsführer


Markus Nowak
Prokurist



ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG

zwischen dem Verantwortlichen

.....
– nachfolgend „Auftraggeber“ genannt –

und dem Auftragsverarbeiter

Bewachungsdienst Dipl.-Kfm. Helmut Ehrl GmbH
Ringbergstr. 1
81673 München

– nachfolgend „Auftragnehmer“ genannt –

– nachfolgend zusammen „Parteien“ genannt –

Diese Anlage und der Auftragsverarbeitungsvertrag korrespondieren mit dem Hauptvertrag zwischen den Parteien.

1. GEGENSTAND DES AUFTRAGS

1.1 Gegenstand des Auftrags:

Der Auftragnehmer erbringt für den Auftraggeber Sicherheitsdienstleistungen. Die konkret erbrachten Leistungen können dem Hauptvertrag zwischen den Parteien entnommen werden. Im Rahmen dieser Leistungen verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers.

1.2 Art und Zweck der Datenverarbeitung:

Art und Zweck der Datenverarbeitung bestimmen sich nach den vom Auftraggeber in Anspruch genommenen Sicherheitsdienstleistungen und dem vereinbarten Leistungsumfang.

Art der Datenverarbeitung: Im Rahmen der Erbringung der Sicherheitsdienstleistungen werden durch den Auftragnehmer Daten erhoben, erfasst, organisiert/geordnet, ausgelesen, abgefragt und verwendet.

Zweck der Datenverarbeitung: Die Datenverarbeitung erfolgt zu folgenden Zwecken

- Verarbeitung personenbezogener Daten zur Auftragsdurchführung (Zutritts-/Zufahrtskontrollen, Legitimationsprüfung, Ausweiserstellung, Kontakt zu Kunden oder Interessenten, Melde- und Berichtswesen etc.)
- Verarbeitung personenbezogener Daten zur Information bei Alarmen (Einbruch, Feuer, technische Störungen, Notrufe, etc.)
- Verarbeitung von und Zugriff auf personenbezogene Daten in der Notruf- und Service-Leitstelle (Zugriff auf Videoüberwachung im Alarmfall, Live-Überwachung)

1.3 Art der Daten:

Im Rahmen der unter 1.1 und 1.2 beschriebenen Datenverarbeitung können die folgenden Datenkategorien verarbeitet werden. Die im Einzelfall relevanten Kategorien bestimmen sich nach den in Anspruch genommenen Leistungen, die im Hauptvertrag zwischen den Parteien definiert werden.

Datenkategorie	Auflistung konkret verarbeiteter Daten
Berufliche Kontakt- und (Arbeits-) Organisationsdaten	Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Personalnummern, Anwesenheit

Private Kontakt- und Identifikationsdaten	Name, Vorname, Geschlecht, Adresse, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Datum und Ort der Geburt, Identifikationsnummern, Nationalität
Positionsdaten	GPS, Funknetz-Ortung, Bewegungsprofil, WLAN-Hotspot-Ortung
Daten zu persönlichen Verhältnissen	Daten zum Ehegatten oder Kindern, Familienstand
Bild- und Videoaufnahmen	Livebilder der Videoüberwachung; Fotoaufnahmen (z.B. im Rahmen der Ausweiserstellung)

1.4 Kreis der Betroffenen:

Im Rahmen der unter 1.1 und 1.2 beschriebenen Datenverarbeitung können die Daten der folgenden Betroffenenkreise verarbeitet werden. Die im Einzelfall relevanten Kategorien bestimmen sich nach den in Anspruch genommenen Leistungen, die im Hauptvertrag zwischen den Parteien definiert werden.

Betroffenengruppe	Beschreibung	Beispiele
Mitarbeiter des Auftraggebers/des Verantwortlichen	Eigene Mitarbeiter des Auftraggebers/ des Verantwortlichen	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
Mitarbeiter anderer Unternehmen	Mitarbeiter anderer Unternehmen, deren personenbezogene Daten für den Auftraggeber/den Verantwortlichen verarbeitet werden	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
Kunden des Auftraggebers/des Verantwortlichen	Jede Person, mit der eine Kunden-Geschäftsbeziehung besteht (mit der jeweiligen verantwortlichen Stelle)	Käufer, Versicherungsnehmer, Mieter, Kunden einer Dienstleistung
Sonstige Geschäftspartner	Jede natürliche Person, mit der eine Geschäftsbeziehung besteht (mit dem Auftraggeber) außer Kunden	Lieferanten, Importeure, Dienstleister, Vermittler, Freelancer

Außenstehende	Jede Person, die in <u>keiner</u> Geschäftsbeziehung mit der jeweiligen Konzerngesellschaft (verantwortlichen Stelle) steht	Besucher, Gäste, Interessenten
---------------	---	--------------------------------

2. DATENSCHUTZBEAUFTRAGTER

Datenschutzbeauftragter des Auftragsnehmers ist:

PROLIANCE GmbH
www.datenschutzexperte.de
 Leopoldstr. 21
 80802 München
datenschutzbeauftragter@datenschutzexperte.de

Bitten nennen Sie bei der Kontaktaufnahme mit dem Datenschutzbeauftragten das Unternehmen, auf welches sich Ihre Anfrage bezieht.

3. UNTERAUFTRAGNEHMER

- ☒ Es werden keine Unterauftragnehmer eingesetzt.
- ☐ Zum Kreis der genehmigten Unterauftragnehmer bei Abschluss dieses Vertrags gehören:

Nr.	Unterauftragnehmer (Name, Anschrift, Ansprechpartner)	Verarbeitete Datenkategorien	Beschreibung der Tätigkeit	Ort der Datenverarbeitung

4. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Die nachfolgenden technischen und organisatorischen Maßnahmen werden zum Zeitpunkt des Vertragsschlusses vereinbart.

4.1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

4.1.1 Zutrittskontrolle

Beschreibung: Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Der Auftragsverarbeiter hat im Rahmen der Zutrittskontrolle folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung/ Liste
Manuelles Schließsystem	Empfang / Rezeption / Pförtner
Sicherheitsschlösser	Besucherbuch / Protokoll der Besucher
Absicherung der Gebäudeschächte	Mitarbeiter- / Besucherausweise
Türen mit Knauf auf Außenseite	Besucher in Begleitung durch Mitarbeiter
Klingelanlage mit Kamera	Sorgfalt bei der Auswahl des Wachpersonals
Videoüberwachung der Eingänge	Sorgfalt bei der Auswahl der Reinigungsdienste

4.1.2 Zugangs- und Zugriffskontrolle

Beschreibung: Das Eindringen Unbefugter in die Datenverarbeitungs(DV)-Systeme (IT-Systeme) ist zu verhindern. Ebenso sind Tätigkeiten in DV-Systemen (IT-Systemen) außerhalb eingeräumter Berechtigungen sowie unerlaubte Zugriffe auf das System von außen zu verhindern.

Der Auftragsverarbeiter hat im Rahmen der Zugangs- und Zugriffskontrolle (zu IT-Systemen) folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Anti-Viren-Software-Server	Erstellen von Benutzerprofilen
Anti-Virus-Software-Clients	Richtlinie „Sicheres Passwort“
Anti-Virus-Software mobile Geräte	Allg. Richtlinie Datenschutz Sicherheit

Firewall	Anleitung „Manuelle Desktopsperre“
Einsatz VPN bei Remote-Zugriffen	Einsatz Berechtigungskonzepte
Sperre externer Schnittstellen (USB)	Minimale Anzahl an Administratoren
Automatische Desktopsperre	Datenschutzraum
Aktenschredder (Schutzklasse 3)	Verwaltung Benutzerrechte durch Administratoren
Externer Aktenvernichter (DIN 66399)	
Physische Löschung und physikalische Vernichtung von Datenträgern	
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	

4.1.3 Trennungskontrolle

Beschreibung: Die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden, muss sichergestellt werden. Maßnahmen zur getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber sind zu gewährleisten.

Der Auftragsverarbeiter hat im Rahmen der Trennungskontrolle folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Physische Trennung (Systeme/ Datenbanken/ Datenträger)	Festlegung von Datenbankrechten

4.1.4 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Beschreibung: Die Pseudonymisierung beschreibt die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Hierfür ist es erforderlich, dass diese zusätzlichen Informationen gesondert aufbewahrt und durch angemessene technische und organisatorische Maßnahmen geschützt werden (Art. 4 Nr. 5 DSGVO).

Der Auftragnehmer hat im Rahmen der Pseudonymisierung folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (mögl. verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

4.2 Integrität. Art. 32 Abs. 1 lit. b DSGVO

4.2.1 Weitergabekontrolle

Beschreibung: Aspekte der Weitergabe personenbezogener Daten sind zu regeln (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern. Maßnahmen zu Transport, Übertragung, Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie zur nachträglichen Überprüfung sind zu treffen.

Der Auftragsverarbeiter hat im Rahmen der Weitergabekontrolle folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Verschlüsselung	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
Einsatz von VPN	Persönliche Übergabe mit Protokoll
Protokollierung der Zugriffe und Abrufe	
Sichere Transportbehälter	
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
Nutzung von Signaturverfahren	

4.2.2 Eingabekontrolle

Beschreibung: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

Der Auftragsverarbeiter hat im Rahmen der Eingabekontrolle folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.3.1 Verfügbarkeitskontrolle

Beschreibung: Die Daten sind gegen zufällige Zerstörung und Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch/logisch).

Der Auftragsverarbeiter hat im Rahmen der Kontrolle zur Verfügbarkeit folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
Serverraum klimatisiert	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
USV	Existenz eines Notfallplans (BCM)
Schutzsteckdosenleisten Serverraum	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	

4.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.4.1 Datenschutz-Management

Beschreibung: Wie wird die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sichergestellt?

Der Auftragsverarbeiter hat im Rahmen des Datenschutz-Managements folgende Maßnahmen ergriffen

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet, ...)	Externer Datenschutzbeauftragter: PROLIANCE GmbH www.datenschutzexperte.de Leopoldstr. 21 80802 München datenschutzbeauftragter@datenschutzexperte.de
Anderweitiges dokumentiertes Sicherheitskonzept	Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.4.2 Incident Response Management

Beschreibung: Technische und organisatorische Maßnahmen, die im Falle eines Datenschutz- oder Cybersicherheitsvorfalls ein angemessenes Schutzniveau gewährleisten.

Der Auftragsverarbeiter hat im Rahmen des Incident Response Managements folgende Maßnahmen ergriffen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Spamfilter und regelmäßige Aktualisierung	Einbindung des Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenpannen
Einsatz von Virens Scanner und regelmäßige Aktualisierung	Dokumentation von Sicherheitsvorfällen und Datenpannen
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Beschreibung:

Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Das heißt, bereits die Werkseinstellungen sollen datenschutzfreundlich ausgestaltet werden. Hierdurch sollen vor allem die Nutzer geschützt werden.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

4.4.4 Auftragskontrolle

Beschreibung: Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Eine Datenverarbeitung durch Dritte (vgl. Art. 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/Datenexporteurs erlaubt. Maßnahmen (technisch und organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur.

Der Auftragsverarbeiter hat im Rahmen der Auftragskontrolle folgende Maßnahmen ergriffen:

Technische Maßnahmen	Organisatorische Maßnahmen
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	Vereinbarung wirksamer Kontrollrechte gegenüber Auftragnehmer



Für den Auftraggeber:

Ort/Datum/Unterschrift

Für den Auftragnehmer:

Marco Ehrl	Markus Nowak
Geschäftsführer	Prokurist

München, 06.05.2025
Ort/Datum/Unterschrift