Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen
Firma
Straße + Hausnummer
PLZ + Ort

– nachfolgend „**Auftraggeber**“ genannt –
und
resin it + office GmbH
Am Dreispitz 6
79589 Binzen

– nachfolgend „**Auftragnehmer**“ genannt –

1. Vertragsgegenstand Im Rahmen der beauftragten Leistungserbringung ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung der beauftragten Leistungen.

2. Gegenstand und Umfang der Beauftragung
2.1Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.
2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in Anlage 1 zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit der Beauftragung.
2.3 Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe der Beauftragung vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass

anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.

2.4Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Hiernach ist der Auftragnehmer insbesondere berechtigt, Informationen über die Nutzung des Dienstes durch den Auftraggeber und seine Mitarbeiter („Nutzungsdaten“) zu erfassen und diese zu Zwecken der Erfüllung der Beauftragung, der bedarfsgerechten Gestaltung des Dienstes, der Bereitstellung von Nutzungsübersichten, der IT- und Datensicherheit und der Fehlerdiagnose und -behebung zu verarbeiten. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

2.5 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Europäischen Union oder ihrer Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des vereinbarten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Pflichten und Rechtsstellung des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal/Vertraulichkeit

5.1 Der Auftragnehmer gewährleistet gemäß Art. 29 DSGVO, dass die ihm unterstellten Personen die Auftraggeber-Daten nach Maßgabe dieses Vertrags sowie den Weisungen des Auftraggebers verarbeiten.

5.2 Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes 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.

6.2 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. Die zum Zeitpunkt des Vertragsschlusses vorhandenen technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 3. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

7.3Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Die Parteien stimmen in diesem Fall überein, dass die Anforderungen der vorstehenden Ziff. 7.3 erfüllt sind, wenn mit dem weiteren Auftragsverarbeiter im Drittstaat die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß Beschluss der EU-Kommission vom 4. Juni 2021 („Standardvertragsklauseln“) abgeschlossen werden. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

8.1Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3 Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.5Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der

Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.
9.2Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1Der Auftragnehmer wird die Auftraggeber-Daten nach Abschluss der Erbringung der Verarbeitungsleistungen löschen, sofern nicht nach dem Recht der Europäischen Union oder ihrer Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 17 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.4Der 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. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten 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 Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.7Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

12.1Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung der erteilten Aufträge. Eine Kündigung des zuletzt auslaufenden Auftrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

13.1Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem jeweiligen Auftrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen

eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.2Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

	Binzen,
Ort, Datum	Ort, Datum
…	…
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

Anlage 1:

Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Ergeben sich aus dem jeweiligen Servicevertrag/ Hauptvertrag.
Art und Umfang der Datenverarbeitung	Ergeben sich aus dem jeweiligen Servicevertrag/ Hauptvertrag.
Art der Daten	• Personenstammdaten • Kommunikationsdaten (z.B. Telefon, E-Mail) • Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) • Kundenhistorie • Vertragsabrechnungs- und Zahlungsdaten • Planungs- und Steuerungsdaten • Auskunftsangaben (von Dritten, z.B. Auskunftsdateien, oder aus öffentlichen Verzeichnissen)
Kategorien betroffener Personen	• Kunden • Interessenten • Abonnenten • Beschäftigte • Lieferanten • Handelsvertreter

	• Ansprechpartner

Technische und organisatorische Maßnahmen (TOM)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

resin it + office GmbH, Am Dreispitz 6, 79589 Binzen
erfüllt diesen Anspruch durch folgende Maßnahmen i.S.d. Art. 32 DSGVO:

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

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒Alarmanlage	☒Schlüsselregelung bzw. -verwaltung/Liste bzw. Dokumentation der Schlüsselvergabe

☒Absicherung der Gebäudeschächte	☒Empfang/Rezeption
☒Zaunanlage	☒Abholung Besucher am Empfang
☒Sicherheitsschlösser	☒Besucher nur in Begleitung durch Mitarbeiter
☒Türen mit Knauf Außenseite	☒Begleitung nach dem Besuch bis zum Ausgang
☒Videoüberwachung	☒Sorgfalt bei Auswahl des Wachpersonals
☒Klingelanlage mit Gegensprechanlage, teilweise mit Kamera	☒Sorgfalt bei Auswahl Reinigungsdienste
	☒Sperrbereiche
☒Automatisches Zugangskontrollsystem	☐Spezielle Schutzvorkehrung für die Aufbewahrung von Back-Ups und/oder sonstige Datenträger
☒Chipkarten/Transpondersysteme (teilweise)	☒Spezielle Schutzvorkehrungen des Serverschranks
☒Schließsystem mit Codesperre	☐

1.2. Zugangskontrolle

Maßnahmen, die geeignet sich zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒Login mit Benutzername + Passwort	☒Verwalten von Benutzerberechtigungen
☒Benutzerkonten über Active Directory	☒Initiale Passwortvergabe
☒Hardware Firewall Server	☒Kennwortverfahren/Richtlinie „Sicheres Passwort Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsinterwall)“
☒BIOS Schutz (separates Passwort)	☒Richtlinie „Löschen/Vernichten“
☒Anti-Viren-Software Server	☒Allg. Richtlinie Datenschutz und/oder Sicherheit
☒Anti-Virus Software Clients	☒Mobile Device Policy
☒Firewall Clients/Laptops	
☒Intrusion Detection Systeme	

☒Mobile Device Management	
☒Einsatz VPN bei Remote-Zugriffen	
☒Verschlüsselung von USB-Sticks	
☒Verschlüsselung Mobile Festplatten	
☒Automatische Desktopsperre	
☒Verschlüsselung von Notebooks/Tablet	

1.3. Zugriffskontrolle:

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒externe Fachkundige Akten- und Datenträgervernichtung gem. DIN 66399	☒Einsatz Berechtigungskonzepte
☒Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒Verwaltung Benutzerrechte durch Administratoren

☒Aktenshredder (Sicherheitsstufe 4 nach DIN 66399))	☒Abschluss von Verträgen zur Auftrags-datenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverar-beitungsanlagen, sofern bei der Fern-wartung die Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
	☒Minimale Anzahl an Administratoren
	☒Richtlinie zur Vernichtung von Dokumenten und Datenträgern

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

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

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

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 technische und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen

☒Daten verschlüsselt	☒Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b. DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒E-Mail-Verschlüsselung mit Anhang, teilweise	☒Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒Einsatz von VPN bei Übermittlung	☒Persönliche Übergabe mit Protokoll
☒Protokollierung der Zugriffe und Abrufe	
☒Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☒Nutzung von Signaturverfahren	
☒Verschlüsselung des Speichermediums von Laptops	

☒Veschlüsselung von CD/DVD-ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)	
☒„Mobile Device Management-System“	

2.2. Eingabekontrolle:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒Übersicht, mit welchen Programmen 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)
☒Zugriffsrechte	☒Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒Klare Zuständigkeiten für Löschungen

	☒Vorgaben zur Aufbewahrung von Formularen, von denen Daten in die automatisierte Verarbeitung übernommen wurden

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

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht um Themen, wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒Feuer- und Rauchmeldeanlagen	☒Backup & Recovery-Konzept
☒Feuerlöscher Serverraum	☒Kontrolle des Sicherungsvorgangs
☒Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☒Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒Einrichtung einer unterbrechungsfreien Stromversorgung (USV)	☒Keine sanitären Anschlüsse im oder oberhalt des Serverraums
☒Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☒Existenz eines Notfallplans (z.B. BSI IT-Grundschutz)
☒Serverraumüberwachung Temperatur und Feuchtigkeit	
☒Back-Up Verfahren (Online)	

☒Serverraum klimatisiert	
☒RAID System/ Festplattenspiegelung	
☒Schutzsteckdosenleisten im Schrank	

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

4.1. Datenschutz-Management

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	☒Bestellung externer Datenschutzbeauftragter Rechtsanwalt Marc E. Evers, DataSEKure Rechtsanwaltsgesellschaft mbH, datenschutz@datasekure.de, Schillerstraße 8, 79102 Freiburg
☒Anderweitiges dokumentiertes Sicherheitskonzept	☒Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
☒Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. Jährlich durchgeführt	☒Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

	☒Datenschutzrichtlinie
	☒Richtlinien/Anweisungen zur Gewährleistung von technsich-organisatorischen Maßnahmen zur Datensicherheit
	☒Verpflichtung der Mitarbeiter auf das Datengeheimnis
	☒Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒Einsatz von Firewall und regelmäßige Aktualisierung	☒Dokumentierter Prozess zur Erkennung und internen Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde)
☒Einsatz von Spamfilter und regelmäßige Aktualisierung	☒Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒Einsatz von Virenscanner und regelmäßige Aktualisierung	☒Einbindung von ☒ DSB und ☒ ISB in Sicherheitsvorfälle und Datenpannen
☒Intrusion Detection System (IDS)	☒Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒Intrusion Prevention System (IPS)	☒Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO):
Privacy by design/Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☒Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	☐

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☒Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☒Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)

☐	☒Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	☒Schriftliche Weisungen an den Auftragnehmer
☐	☒Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☒Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	☒Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☒Regelung zum Einsatz weiterer Subunternehmer
☐	☒Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrages
☐	☒Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 3 – Weitere Auftragsverarbeiter

Firma (Unterauftragnehmer)	Kontaktdaten	Leistung
DocuWare GmbH Planegger Str. 1 82110 Germering	Geschäftsführer: Dr. Michael Berger, Max Ertl +49 89 8944330 docuware@docuware.com	Basissoftware, Lizenzen und Dienstleistung
Ricoh RICOH DEUTSCHLAND GmbH Vahrenwalder Str. 315 30179 Hannover	Geschäftsführer: Michael Raberger + 49 511 67420 info@ricoh.de	DocuWare Dienstleistung
Adminox GmbH & Co. KG Hauptstr. 23 79288 Gottenheim	vertreten durch: Yannic Wintermantel +49 761 7678700 beratung@adminox.de	DocuWare Dienstleistung
DocuScan GmbH Schloss Buschfeld 50374 Erftstadt	Vertreten durch: Michael Bochmann, Stefan Schmidt +49 2235 9789850 info@docuscan.de	DocuWare Erweiterungen
Natif.ai GmbH Campus Starterzentrum Gebäude A1 1 66123 Saarbrücken	Geschäftsführer: Dr. Michael Berger, Johannes Korves +49 681 30264901 contact@natif.ai	DocuWare KI
Mirantis 900 E Hamilton Avenue Suite 650 Campbell CA 95008	CEO: Alex Freedland +1 650 9639828	OnPremise Modul Intellix
Werner Tantzky GmbH Johann-Georg-Schlosser-Straße 21 + 23 76149 Karlsruhe	Geschäftsführer: Mirko Tantzky +49 721 985890 info@tantzky.de	Schnittstelle ABAS

PROWIS Automatisierung GmbH Alter Holzhafen 21a 23966 Wismar	Geschäftsführer: Dipl.-Ing. Hartmut Frank +49 3841 6620230 info@prowis.de	Schnittstelle DATEV
Itarius UG (haftungsbeschränkt) Friedrich-Hebbel-Str. 3 95032 Hof	Geschäftsführer: Roger Goetzendorff +49 9281 8184418 info@itarius.com	Schnittstelle divers
Steigauf Daten Systeme GmbH Otto-Hahn-Str. 13a 85521 Riemerling	Vertreten durch: Roul Steigauf +49 89 411186210 kundenservice@steigauf.de	Schnittstelle divers
Inway Systems GmbH Edisonallee 3 89231 Neu-Ulm	Geschäftsführer: Matthias Schuster, Michael Maier +49 731 8800730 info@Inway.de	Schnittstelle Dynamics
prisma informatik GmbH Frankenstraße 146 90461 Nuremberg	CEO: Claudius Malue and Jens Thamer +49 911 23980550 info@prisma-informatik.de	Schnittstelle NAV/BC
Fellowmind Germany GmbH Technologiepark 8 33100 Paderborn	Geschäftsführer: Anje Hickey, Michael Scheibe, Thorsten Brombach + 49 52 51161920 info@fellowmind.de	Schnittstelle NAV/BC
WEKO eSolutions GmbH Fanny-Zobel-Str. 09 12435 Berlin	CEO: Werner Kopmann +49 30 53621026 info@weko.de	Schnittstelle Sage
Datatronic Software AG Willy-Brandt-Ring 4 67592 Flörsheim-Dalsheim	Vorstand: Pascal Bühler +49 6241 7070100 info@datatronic.de	Schnittstelle Sage
Varelmann Beratungs Gesellschaft mbH Im Technologiepark 6 26129 Oldenburg	Vertreten durch: Gerrit Ellinghausen, Jochen Retzkowski, Lars Sonka, Georg Varelmann +49 441 779170 info@varelmann.de	Schnittstelle SAP
penoTEC Aktiengesellschaft Carl-Zeiss-Str. 11 79761 Waldshut-Tiengen	Vorstand: Peter Spiegelhalter +49 7741 838390 info@penotec.de	Schnittstellen divers
VALIDATED ID S.L C/ Sepúlveda 143, 4º2ª ES-08011 Barcelona	Vorsitzender: Santi Casas +34 900828948 info@validatedid.com	Signaturen

Celonis SE Theresienstr. 6 80333 Munich	Martin Klenk, Bastian Nominacher, Alexander Rinke +49 89 416159670 info@celonis.com	Verarbeitungsplattform MAKE
VD2 GmbH Singapurstraße 15 20457 Hamburg	Vertreten durch: Nadine Rauß +49 179 2977263 emails@vd2.software	Verfahrensdokumentation