Vertrag über die Auftragsverarbeitung nach Artikel 28 DS-GVO

zwischen (Verantwortlicher, nachstehend Auftraggeber genannt)

vertreten durch

und (Auftragsverarbeiter, nachstehend Auftragnehmer genannt)

resin it + office GmbH
79589 Binzen, Am Dreispitz 6
vertreten durch Friedrich Resin, Geschäftsleitung

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem mit dem Auftraggeber geschlossenen Servicevertrag.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Artikel 4 Nr. 2 und Artikel 28 DS-GVO auf Grundlage dieses Vertrages.

1.2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Servicevertrags/Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten (entsprechend der Definition von Artikel 4 Nr. 2 DS-GVO)

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Servicevertrag/Hauptvertrag.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.2. Art der personenbezogenen Daten (entsprechend der Definition von Artikel 4 Nr. 1,13,14 und 15 DS-GVO)

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- 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)

2.3. Kategorien betroffener Personen (entsprechend der Definition von Artikel 4 Nr. 1 DS-GVO)

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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

3.2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

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

3.4. Der Auftraggeber ist berechtigt, sich wie unter Ziffer 5 und 6 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

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

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

4.1. Weisungsberechtigte Personen des Auftraggebers sowie von resin als Auftragnehmer sind die jeweiligen Geschäftsführer oder deren Beauftragte

4.2. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

5.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine

solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Artikel 28 Abs. 3 Satz 2 lit. a DS-GVO)

5.2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

5.3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Massnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

5.5. Bei der Erfüllung der Rechte der betroffenen Personen nach Artikel 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Artikel 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

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

5.7. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

5.8. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

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

5.10. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

5.11. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, die vom Auftraggeber schriftlich definierten Geheimnisschutzregeln zu beachten.

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

5.13. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Artikel 28 Abs. 3 Satz 2 b und Artikel 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

5.14. Sofern anwendbar: Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Artikel 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Artikel 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artikel 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artikel 38 und 39 DS-GVO ausübt.
   - Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
   - Als externer Datenschutzbeauftragter ist beim Auftragnehmer Herr Marc E. Evers, www.datasekure.de, E-Mail: datenschutz@resin.de, bestellt.
   - Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
   - Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 11 dieses Vertrages.

7. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Artikel 33 und Artikel 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Artikel 33 und 34 DS-GVO angemessen zu unterstützen (Artikel 28 Abs. 3 Satz 2 f DS-GVO). Meldungen nach Artikel 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziffer 4 dieses Vertrages durchführen.

8. Unterauftragsverhältnisse (Artikel 28 Abs. 3 Satz 2 lit. D DS-GVO)

8.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der

Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

8.2. Der Auftragnehmer darf Unterauftragsnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der unter Anlage 2 genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig soweit die in dieser Vereinbarung zugesicherten Vorkehrungen nicht unterschritten werden.

8.3. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

8.4. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

8.5. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Artikel 28 Abs. 4 und Abs. 9 DS-GVO).

8.6. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Artikel 29 und Artikel 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

8.7. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

9. Technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO (Artikel 28 Abs. 3 Satz 2 lit. c DS-GVO)

9.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Artikel 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

9.2. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

9.3. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

9.4. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen sowie die vereinbarten Standards nicht unterschritten werden.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

10. Berichtigung, Einschränkung und Löschung von Daten

10.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

10.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

11. Kontrollrechte des Auftraggebers

11.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

11.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Artikel 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

11.3. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

12. Mitteilung bei Verstößen des Auftragnehmers

12.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

12.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

13. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Artikel 28 Abs. 3 Satz 2 lit. g DS-GVO

13.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

13.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmern gelangte Daten, Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen

13.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

14. Haftung

Auf Artikel 82 DS-GVO wird verwiesen. Weitere Regelungen sind im Servicevertrag/Hauptvertrag vereinbart.

15. Sonstiges

15.1. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

15.2. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15.4. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum	Auftraggeber (Unterschrift)
Ort, Datum	Auftragnehmer (Unterschrift)

Anlage 1 - Technische und organisatorische Maßnahmen (TOM)

Stand: 2021/ Letzte Aktualisierung: 10.06.2021

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

Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz, Pförtner, Alarmanlagen, Videoanlagen etc.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Alarmanlage	☒	Rezeption
☒	Chipkarten / Transpondersystem	☒	Besuch nur in Begleitung
☒	Automatisches Zugangskontrollsystem	☒	Schlüsselregelung Dokumentation / Liste
☒	Klingelanlage mit Gegensprechanlage	☒	Auswahlsorgfalt Reinigungsdienst
☒	Klingelanlage, teils mit Kamera	☐	
☒	Schließsystem mit Codesperre	☐	
☒	Sicherheitsschlösser	☐	
☒	Türen mit Knauf Außenseite	☐	
☐		☐	

Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Login mit Benutzername und Passwort	☒	Richtlinie „Sicheres Passwort“
☒	Firewall Clients / Laptops	☒	Allg. Richtlinie Datenschutz und IT-Sicherheit
☒	Anti-Viren-Software Clients	☒	Richtlinie „Löschen / Vernichten“
☒	Automatische Desktopsperre	☒	Initiale Passwortvergabe
☒	Anti-Viren-Software Server	☒	Verwalten von Benutzerberechtigungen
☒	Intrusion Detection Systeme (Angriffserkennung)	☒	Richtlinie Sicherheit Mobiles (Mobil Device Policy)
☒	Hardware Firewall Server	☐	
☒	Benutzerkonten über Active Directory	☐	
☒	Intrusion Detection Systeme (Angriffserkennung)	☐	
☒	Benutzerkonten über Active Directory	☐	
☒	Mobile Device Management	☐	
☒	Einsatz VPN bei Remote-Zugriffen	☐	
☒	Verschlüsselung USB-Sticks	☐	
☒	Verschlüsselung Mobile Festplatten	☐	
☒	Verschlüsselung Notebooks / Laptops	☐	
☒	BIOS Schutz (separates Passwort)	☐	
☐		☐	

Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Aktenschredder Sicherheitsstufe 4 nach DIN 66399	☒	Richtlinie zur Vernichtung von Dokumenten und Datenträgern
☒	Externe Aktenvernichtung nach DIN 66399	☒	Verwaltung Benutzerrechte durch Administratoren
☒	Externe Datenvernichtung (Löschung von Datenträgern) nach DIN 66399	☐	
☒	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐	
☐		☐	

Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing (Sichere Testumgebung) etc.

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

Pseudonymisierung
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Daten verschlüsselt	☒	Interne Anweisung, personenbezogene Daten (Weitergabe, Löschfrist, Pseudonymisierung)
☐		☐	

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

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	E-Mail-Verschlüsselung mit Anhang, teilweise	☒	Persönliche Übergabe mit Protokoll
☒	Einsatz von VPN bei Übermittlung	☒	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒	Protokollierung der Zugriffe und Abrufe	☐	
☒	Bereitstellung über verschlüsselte Verbindungen	☐	

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Nutzung von Signaturverfahren, teilweise	☐	
☐		☐	

Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

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
☐		☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐		☒	Vorgaben zur Aufbewahrung von Formularen, von denen Daten in die automatisierte Verarbeitung übernommen wurden
☐		☒	Klare Zuständigkeiten für Löschungen
☐		☐	

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

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Feuer- und Rauchmeldeanlagen	☒	Backup & Recovery-Konzept
☒	Feuerlöscher Serverraum	☒	Kontrolle des Sicherungsvorgangs
☒	Serverraumüberwachung Temperatur und Feuchtigkeit	☒	Existenz eines Notfallplans (z.B. BSI IT-Grund-Schutz)
☒	Serverraum klimatisiert	☒	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒	Schutzsteckdosenleisten Serverraum	☐	
☒	USV	☐	
☒	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☐	
☒	Storage-System (RAID/ Festplattenspiegelung	☐	
☒	Online Backup		
☒	Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐	
☐		☐	

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

Datenschutz Management

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	☒	Interner / externer Datenschutzbeauftragter Vanessa Egle, datenschutz@resin.de 07762 / 708860
☒	Anderweitiges dokumentiertes Sicherheits-Konzept	☒	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 Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
☐		☒	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐		☐	

Incident-Response-Management
Unterstützung bei der Reaktion von Sicherheitsverletzungen und Datenschutzverletzungen

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Einsatz von Firewall und regelmäßige Aktualisierung	☒	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (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 Sicherheitsvor-fällen und Datenpannen
☐		☐	

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

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Es werden nicht mehr personen-bezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐	
☒	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maß-nahmen	☐	
☐		☐	
☐		☐	

Auftragskontrolle (Outsourcing an Dritte)
Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

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 Daten-schutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐		☒	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐		☒	Regelung zum Einsatz weiterer Sub- Unternehmer
☐		☒	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐		☒	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anlage 2 – Genehmigte Unterauftragnehmer

Firma (Unterauftragnehmer)	Kontaktdaten	Leistung