

Anhang

Rahmenvereinbarung über die Bereitstellung und den Betrieb einer E-Mail-Versand-Dienstleistung

zwischen

4OfficeAutomation GmbH, Schlägelweg 46a,
31275 Lehrte,

nachfolgend "4OA" genannt,

cobra computer's brainware GmbH,
Weberinnenstraße 7, 78467 Konstanz,

nachfolgend "cobra" genannt, und

Firma:	OEKOGENO eG
Ansprechpartner:	Rainer Schüle
Straße:	Herrenstraße 45
PLZ/Ort:	79098 / Freiburg Im Breisgau
Telefon:	0761 383885 0
Telefax:	0761 383885 51
E-Mail:	schuele@oekogeno.de

nachfolgend „Kunde“ genannt.

§ 1 Vertragsgegenstand

Die nachfolgenden Vereinbarungen regeln die Rahmenbedingungen für die Bereitstellung des Zugriffs auf die Funktionalitäten der im Folgenden näher beschriebenen Software-as-a-Service (SaaS)-Lösung „News & Mail Service für cobra“ von 4OA über eine Schnittstelle. Mittels dieser Schnittstelle erhält der Kunde die technische Möglichkeit und Berechtigung auf die Service-Plattform „News & Mail Service für cobra“ von 4OA zuzugreifen und im Rahmen dieses Vertrages zu nutzen. Die Bestellung dieser Lösung erfolgt jeweils mittels Einzelbestellung (auch per E-Mail möglich) nach Maßgabe dieser Rahmenvereinbarung.

§ 2 Rechte und Pflichten

1. Rechte und Pflichten von 4OA

- 4OA stellt die Service-Plattform „News & Mail Service für cobra“ bereit. Hierbei handelt es sich um eine technische, internetbasierte Plattform für den Versand von E-Mails, die auf einem oder mehreren von 4OA in Deutschland bereitgestellten Server(n) betrieben wird. Zusätzlich sind Funktionen zur Erstellung der E-Mails, der Verwaltung von Benutzern sowie zur Erstellung von Statistiken integriert. Die Leistung wird nachfolgend auch als „Dienstleistung“ bezeichnet.
- 4OA ist ausschließlich Übermittler von E-Mails und nicht für den Inhalt der durch die Dienstleistung

versendeten E-Mails verantwortlich. 4OA führt für alle zu versendenden E-Mails mehrfache Zustellversuche durch. Mangels Einflusses auf das Verhalten der Empfänger und Empfängerserver kann jedoch für eine erfolgreiche Zustellung keine Gewährleistung übernommen werden.

- Während der gesamten Vertragsdauer wird 4OA die jeweils aktuelle Version von „News & Mail Service für cobra“ Instand halten. Ein Anspruch auf bestimmte Erweiterungen oder Ergänzungen der Software besteht nicht. Die Nutzbarkeit der Software wird gemäß der Leistungsbeschreibung (durch Wartung und Pflege der Software sowie durch Bereitstellung neuer Software-Versionen) mit einer Erreichbarkeit von 98 % sichergestellt.

2. Rechte und Pflichten von cobra

- cobra stellt dem Kunden aus der Software cobra CRM mittels einer Schnittstelle Zugriff auf die Dienstleistung „News & Mail Service für cobra“ von 4OA zur Verfügung. Hierfür werden cobra oder 4OA für jeden Kunden ein eigenes Nutzerkonto anlegen.
- cobra und 4OA sind verpflichtet, die Dienstleistung nur Kunden zur Verfügung zu stellen, die sich registriert haben, volljährig und geschäftsfähig sind oder mit Zustimmung ihrer gesetzlichen Vertreter handeln.

3. Rechte und Pflichten des Kunden

- cobra räumt dem Kunden gegen Entgelt das nicht ausschließliche, auf die Laufzeit dieses Vertrages zeitlich beschränkte Recht ein, auf „News & Mail Service für cobra“ in der jeweils aktuellen Version mittels Internet zuzugreifen und die verbundenen Funktionalitäten zur Durchführung von E-Mail-Marketing-Aktionen gemäß diesem Vertrag zu nutzen. Die Bereitstellung des Zugangs des Kunden zum Internet ist ausdrücklich nicht Teil der Leistung.
- Der Kunde muss den Teilnahmeregeln (Anhang A), die Bestandteil dieses Vertrages sind, zugestimmt haben, um die Dienstleistung nutzen zu dürfen. 4OA ist berechtigt, unverzüglich und ohne vorherige Ankündigung die Bereitstellung der Dienstleistung an solche Kunden zu verweigern oder einzustellen, die gegen die Teilnahmeregeln verstoßen oder verstoßen haben.
- Der Kunde wird die ihm bzw. den Nutzern zugeordneten Nutzungs- und Zugangsberechtigungen sowie Identifikations- und Authentifikations-Sicherungen vertraulich behandeln und dafür sorgen, dass kein Unbefugter davon Kenntnis erlangt oder sie nutzen kann. Sobald der Kunde Kenntnis davon erlangt, dass Letzteres geschehen ist, informiert er cobra hiervon unverzüglich in Textform.
- Der Kunde wird dafür Sorge tragen, dass (z.B. bei der Übernahme von Texten und Daten Dritter auf den Server) alle gewerblichen Schutz- und Urheberrechte beachtet werden.
- Der Kunde wird „News & Mail Service für cobra“ nicht missbräuchlich nutzen oder nutzen lassen, insbesondere keine Informationsangebote mit rechts- oder sittenwidrigen Inhalten übermitteln.

§ 3 Vergütung

1. Die vom Kunden zu entrichtende Vergütung entspricht der unter www.cobra.de abrufbaren cobra Preisliste, die Bestandteil dieses Vertrages ist, in der jeweils gültigen Fassung.

Vertragsgebühr

Die monatliche Vertragsgebühr errechnet sich gemäß aktueller Preisliste zum Zeitpunkt der jeweiligen Einzelbestellung. Sie kann sich bei Änderung der Anzahl der Adressen bzw. bei Änderung der cobra Preisliste nach § 4 Abs. 1, 2 verändern. Die Rechnungsstellung und Abbuchung erfolgt monatlich jeweils zu Beginn eines Kalendermonats.

	Anzahl Mails pro Monat	Monatlicher Preis netto (EUR)	Summe (EUR)
News & Mail Service für cobra	10000	49,00 €	49,00 €
zzgl. jeweilige gesetzliche MwSt. (bei Vertragsschluss 19 %)			9,31 €
Monatliche Vertragsgebühr			58,31 €

Ermächtigung zum Bankeinzug

Der Kunde ermächtigt cobra die monatliche Vertragsgebühr von folgendem Konto abzubuchen:

Bank	
Kontoinhaber	
IBAN	
BIC	

2. Bei Änderung der Anzahl der maximal zulässigen E-Mails innerhalb der Laufzeit wird die dadurch entstehende geänderte Vergütung ab dem Änderungsdatum fällig.
3. Die vertraglich vereinbarte Vergütung ist jeweils im Voraus für den nächsten Kalendermonat zu bezahlen. Die Vergütung für den ersten Monat ist bei Eingang der jeweiligen Einzelbestellung zu bezahlen. Der Betrag wird von cobra per Bankeinzug vom Konto des Kunden abgebucht.
4. Zu der zu berechnenden Vergütung tritt die jeweils geltende Umsatzsteuer hinzu.
5. Während eines Zahlungsverzugs durch den Kunden in nicht unerheblicher Höhe ist cobra berechtigt, den Zugang zum „News & Mail Service für cobra“ zu sperren. Rücklastschriftkosten für nicht eingelöste Bankeinzüge trägt der Kunde.

§ 4 Vertragslaufzeit und Beendigung

1. Die Mindestvertragsdauer dieses Rahmenvertrages beträgt 1 Kalendermonat ab Vertragsabschluss (Datum der Unterschrift). Danach kann der Vertrag vom Kunden, 4OA oder cobra mit einer Kündigungsfrist von 30 Tagen zum Monatsende, frühestens jedoch zum Ablauf der Laufzeit der jeweiligen Einzelbestellung schriftlich gekündigt werden (es gilt das Datum des Poststempels).
2. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn eine oder mehrere wesentliche

Vereinbarungen durch eine Partei nicht eingehalten werden und nach einer schriftlichen Aufforderung zur Besserung diese nicht innerhalb einer Frist von 14 Tagen erfolgt ist sowie das Nichtverschulden nicht ausreichend nachgewiesen wurde. Für cobra besteht ferner ein außerordentlicher Kündigungsgrund bei einem Zahlungsverzug von mehr als 2 Monaten.

3. Bei einer Erhöhung der Nutzungsvergütung gemäß cobra Preisliste hat der Kunde ein Sonderkündigungsrecht innerhalb von 14 Tagen nach Rechnungserhalt.
4. Jede Kündigung bedarf der Textform.
5. Die Einzelbestellungen haben die in der jeweiligen Bestellung vom Kunden angegebene feste Laufzeit. Eine Einzelbestellung kann jeweils nur für volle Kalendermonate erfolgen. Die Mindestlaufzeit für eine Einzelbestellung beträgt 1 Kalendermonat. Eine Einzelbestellung ist nur bei Bestehen dieses Rahmenvertrages möglich.

§ 5 Datenschutz

1. 4OA speichert bei der Nutzung der Dienstleistung folgende Daten für üblicherweise ein Jahr:
 - a. Den Inhalt der E-Mail.
 - b. Die IP-Adresse des Kunden zum Zeitpunkt des Versands eines Mailings.
 - c. Die Liste der Empfänger samt aller Personalisierungsdaten.
 - d. Die Versandergebnisse
 - e. Statistiken, insbesondere auch Statistiken zu Klicks, Öffnungen und Abmeldungen.
2. Der Kunde nimmt zur Kenntnis, dass eine Vertraulichkeit seiner Daten nur dann gewährleistet werden kann, wenn er die ihm mitgeteilten Zugangsdaten vertraulich behandelt und nicht an Dritte weitergibt, und Dritten keinen Zugang zu seinem System gewährt. Sollten die Daten verloren gehen oder der Kunde Kenntnis davon haben, dass Unbefugten möglicherweise Kenntnis dieser Daten haben könnten, so muss der Kunde 4OA oder cobra unverzüglich davon in Kenntnis setzen, damit 4OA die unbefugte Nutzung unterbinden kann.
3. Zu Zwecken der technischen Analyse und der Fehlerbehebung hat 4OA das Recht, in die Daten des Kunden Einblick zu nehmen, auch ohne den Kunden hiervon in Kenntnis zu setzen.
4. 4OA verpflichtet sich, den Datenschutz im Sinne des Bundesdatenschutzgesetzes zu gewährleisten und die Daten des Kunden nicht an Dritte weiterzugeben oder für in diesem Vertrag nicht definierte Zwecke zu nutzen.
5. Zwischen 4OA und dem Kunden wurde eine Vereinbarung zur Auftragsverarbeitung getroffen (Anhang B), die Bestandteil dieses Vertrages ist.

§ 6 Übertragung

Der Vertrag kann von 4OA oder cobra mit Zustimmung des jeweils anderen auf eine andere juristische Person übertragen werden, die die aus dem Vertrag hervorgehenden Rechte und Pflichten ggü. dem Kunden übernimmt.

§ 7 Salvatorische Klausel

Sollte eine Bestimmung dieses Vertrages ganz oder teilweise unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten

sich, anstelle einer unwirksamen Bestimmung eine dieser Bestimmung möglichst nahekommende Regelung zu treffen.

§ 8 Sonstiges

1. Gerichtsstand ist die Stadt Hannover in der Bundesrepublik Deutschland.
2. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
3. Änderungen bedürfen der Textform.

Anhänge

- A) Teilnahmeregeln der 4OfficeAutomation GmbH für „News & Mail Service für cobra“
 - B) Auftragsverarbeitung gemäß Art. 28 AB. 3 DS-GVO
 - C) Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO für den „News & Mail Service“ der 4OfficeAutomation GmbH
-
-

Anhang A:

Teilnahmeregeln der 4OfficeAutomation GmbH für „News & Mail Service für cobra“

1. Ausschließlich der Ersteller und Versender, im Folgenden „Anwender“ genannt, ist für den Inhalt der E-Mails verantwortlich.
2. Der Anwender verpflichtet sich, E-Mails nur an Empfänger zu verschicken, die hierzu ihre Einwilligung erteilt haben (siehe §7 UWG). Die Zustimmung des Empfängers muss dokumentiert vorliegen und cobra oder 4OA auf Verlangen ausgehändigt werden.
3. Der Anwender hat auf Aufforderung von 4OA oder von cobra darzulegen, auf welche Weise die E-Mail-Adressen von Empfängern gesammelt worden sind.
4. Der Anwender ist verpflichtet, in den zu versendenden E-Mails folgende Angaben zu machen:
 - a. Der Grund für den Versand des E-Mails.
 - b. Impressum mit Namen und Firmennamen des Anwenders und vollständiger Kontaktinformation (siehe §5 Absatz 1 TMG).
 - c. Werbesendungen sind als solche kenntlich zu machen.
 - d. Eine Möglichkeit, sich ohne Kenntnisse von Zugangsdaten von zukünftigen E-Mails abzumelden.
5. E-Mails, die einen der folgenden Inhalte enthalten, dürfen nicht versendet werden:
 - a. Angebote oder Links zu Angeboten, die in der Europäischen Union oder dem Land des Adressaten gesetzlich verboten sind, wie beispielsweise illegale Software, Cracks, Raubkopien, MP3s, DVDs, illegale Betäubungsmittel.
 - b. Radikale, betrügerische, rassistische, beleidigende, pornografische, verleumderische, gewaltverherrlichende oder sonst wie gegen die guten Sitten verstoßende Inhalte.
 - c. Nachweislich unseriöse Angebote, insbesondere solche, die gegen das Gesetz gegen unlauteren Wettbewerb verstoßen.
 - d. Inhalte, die gegen die Bestimmungen des Jugendschutzgesetzes verstoßen.
 - e. Absichtlich irreführende Inhalte, wie z.B. eine irreführende Absender- oder Betreffzeile, die den Inhalt oder die Herkunft einer E-Mail verschleiern sollen.
 - f. Viren, Skripte oder ähnlich potentiell gefährliche Inhalte.
6. Für die Bereitstellung von Bildern, Dateianhängen sowie zur Erstellung von E-Mails und den Adressimport ist es dem Anwender möglich, Dateien auf die Server vom 4OA zu laden. Der Anwender übernimmt die volle Verantwortung und Haftung für alle Daten, die er auf den Server lädt, und verpflichtet sich, keine Daten auf einen Server von 4OA zu laden, die
 - a. Viren enthalten
 - b. Gegen das Urheberrecht verstoßen
 - c. Sonstige illegale, sittenwidrige oder die Dienstleistung gefährdende Inhalte.
7. Der Anwender hat Kenntnis davon zu nehmen, dass der Versand von E-Mails den Rechtsordnungen der jeweiligen Staaten, in denen der Empfänger seinen Sitz oder Aufenthaltsort hat, unterliegen kann und verpflichtet sich, die in selbigen Staaten geltenden Gesetze und Vorschriften zu beachten, d.h. er darf keine E-Mails versenden, die gegen solche gesetzlichen Rechte oder Vorschriften verstoßen.
8. Der Versand von Spam-E-mails ist nicht gestattet.
9. Anwender, die gegen eine oder mehrere Teilnahmeregeln verstoßen, können von cobra oder 4OA unverzüglich und ohne vorherige Ankündigung temporär oder dauerhaft von der Nutzung der Dienstleistung ausgeschlossen werden.
10. 4OA behält sich vor, die Inhalte von E-Mails, die durch die Software versendet worden sind oder versendet werden sollen, stichprobenartig zu überprüfen.
11. 4OA hat das Recht, bei jedem Versand eines E-Mails die IP-Adressen des Anwenders für die Dauer von üblicherweise einem Jahr zu speichern.
12. Der Anwender nimmt zur Kenntnis, dass aufgrund gesetzlicher Verpflichtungen E-Mail-Adressen, an die aufgrund eines sog. Hardbounces dauerhaft keine E-Mails zugestellt werden können, vom 4OA auf eine Do-Not-E-Mail-List gesetzt und von künftigen Zustellversuchen ausgeschlossen werden. Das gleiche gilt für die E-Mail-Adressen von Empfängern, von denen Beschwerden vorliegen.
13. Bei Vorliegen von Beschwerden ist 4OA berechtigt, die Versendung weiterer E-Mails des Anwenders ohne vorherige Ankündigung zu unterbinden und das Nutzerkonto ggf. kostenpflichtig nach eigenem Ermessen zu sperren.
14. Datenspeicherung und Datensicherheit: 4OA speichert bei der Nutzung der Dienstleistung folgende Daten für üblicherweise ein Jahr:
 - a. Den Inhalt der E-Mail.
 - b. Die IP-Adresse des Anwenders zum Zeitpunkt des Versands eines Mailings.
 - c. Die Liste der Empfänger samt aller Personalisierungsdaten.
 - d. Die Versandergebnisse
 - e. Statistiken, insbesondere auch Statistiken zu Klicks, Öffnungen und AbmeldungenDaten von Abmeldungen und Beschwerden (E-Mail-Adresse des Empfängers, Datum, IP, Nutzer ID) werden üblicherweise dauerhaft gespeichert, um den gesetzlichen Vorschriften des UWG (insbesondere §7 3.3) zu genügen.
15. Der Anwender nimmt zur Kenntnis, dass eine Vertraulichkeit seiner Daten nur dann gewährleistet werden kann, wenn er die ihm mitgeteilten Zugangsdaten vertraulich behandelt und nicht an Dritte weitergibt, und Dritten keinen Zugang zu seinem System gewährt. Sollten die Daten verloren gehen oder der Anwender Kenntnis davon haben, dass Unbefugten möglicherweise Kenntnis dieser Daten haben könnten, so muss der Anwender 4OA oder cobra unverzüglich davon in Kenntnis zu setzen, damit 4OA die unbefugte Nutzung unterbinden kann.
16. Zu Zwecken der technischen Analyse und der Fehlerbehebung hat 4OA das Recht, in die Daten des Anwenders Einblick zu nehmen, auch ohne den Anwender hiervon in Kenntnis zu setzen.
17. 4OA verpflichtet sich, den Datenschutz im Sinne des Bundesdatenschutzgesetzes zu gewährleisten und die Daten des Anwenders nicht an Dritte weiterzugeben oder für in diesem Vertrag nicht definierte Zwecke zu nutzen.

Stand: 17.04.2018

Anhang B:

Auftragsverarbeitung gemäß Art. 28 AB. 3 DS-GVO

zwischen dem Kunden

Firma:	OEKOGENO eG
Ansprechpartner:	Rainer Schüle
Straße:	Herrenstraße 45
PLZ/Ort:	79098 / Freiburg Im Breisgau
Telefon:	0761 383885 0
Telefax:	0761 383885 51
E-Mail:	schuele@oekogeno.de

(Auftraggeber)

gegenüber der

4OfficeAutomation GmbH, Schlägelweg 46a, 31275 Lehrte,
HRB 203395, Amtsgericht Hildesheim
(Auftragnehmer)

1. Gegenstand und Dauer des Auftrags

Der Gegenstand des Auftrags zum Datenumgang umfasst die Erstellung von E-Mail Newslettern sowie deren Übermittlung an benannte Empfängeradressen, jeweils in dem vom Auftraggeber festgelegten Umfang. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten

- (1) Die zu verarbeitenden Daten beinhalten insbesondere Listen von Empfängern eines E-Mail Newsletters sowie dazugehörige Personalisierungsdaten in einem vom Auftraggeber nach eigenem Ermessen festgelegten Umfang, sowie durch Verarbeitung des Auftrags anfallende Protokolldaten.
- (2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der

Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

- (3) 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 nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

- (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.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Hierfür anfallende Kosten werden vom Auftraggeber getragen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- (1) **Datenschutzbeauftragter** Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Johannes Vorwerk, Geschäftsführer, Tel. 05132/946 7012, E-Mail jvorwerk@mynewsletter.rocks benannt.
- (2) **Vertraulichkeit** Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- (3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage C]
- (4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- (5) 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.

- (6) 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. Hierfür anfallende Kosten werden vom Auftraggeber getragen.
- (7) 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.

6. Unterauftragsverhältnisse

- (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 Telekommunikations- oder Hosting Leistungen, 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.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

7. Kontrollrechte des Auftraggebers

- (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.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 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.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

- (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-Folgeabschätzung
 - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

- (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.
- (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 gelangten

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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

- (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.

Anhang C:

Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO für den „News & Mail Service“ der 4OfficeAutomation GmbH

Zur Gewährleistung des Schutzes von Kundendaten ergreift die 4OfficeAutomation GmbH (im Nachfolgenden als „Anbieter“ bezeichnet) die folgenden technischen und organisatorischen Maßnahmen:

- (1) Verschlüsselung personenbezogener Daten
 - HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport)
- (2) Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
 - Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern
 - Berechtigte können nur auf für sie berechnete Daten zugreifen
 - Personenbezogene gespeicherte Daten können nur im Rahmen des Berechnungskonzepts gelesen, kopiert, verändert oder entfernt werden
 - Verwendung fortlaufend aktualisierter Virenschutzsoftware
 - Schutz des E-Mail-Verkehrs vor Viren und Spam
 - Firewallsysteme
 - Verwendung getesteter Software
 - Trennung der Produktiv- von der Test- und Entwicklungsumgebung
 - Verpflichtung der Mitarbeiter auf das Datengeheimnis
 - Klimaanlage in Serverräumen
 - Hohe Passwortsicherheit
 - Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums
 - Während der Geschäftszeiten Zutritt zu Geschäftsräumen durch Mitarbeiter kontrolliert
 - Besucher der Rechenzentren werden begleitet
 - Festlegung der berechtigten Personen in Listen für die sensiblen Bereiche der Rechenzentren
 - Definierter Kreis von Zugangsberechnigten
 - Sichere Löschung von Datenträgern
 - Verbot der Nutzung privater Datenträger
 - Empfang besetzt während Geschäftszeiten
 - Brandschutzvorrichtungen
- (3) Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
 - Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten)
 - Datensicherungs- und Recoverykonzept
 - Personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch regelmäßiges Backup
 - Sicherheitskopien
 - Unterbrechungsfreie Stromversorgung
 - Redundante Stromzuführungen
 - Überwachungs- und Meldesysteme
- (4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung
 - Regelmäßige Prüfung, ob / in welchem Umfang Zugangsrechte noch erforderlich sind
 - Incident-Response-Management
 - Auftragskontrolle bei Auftragsverarbeitung
 - Durchführung von notwendigen Anpassungsmaßnahmen