

Anhang A:

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

1. Verantwortlichkeit

- (1) Ausschließlich der Ersteller und Versender, im Folgenden „Anwender“ genannt, ist für den Inhalt der E-Mails verantwortlich.
- (2) Der Versender ist dafür verantwortlich, dass der Versand rechtmäßig erfolgt und insbesondere die Inhalte der versendeten E-Mails nicht gesetzlichen Verboten und Geboten zuwiderlaufen.
- (3) 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.

2. Einwilligung

- (1) Der Anwender verpflichtet sich, E-Mails nur an Empfänger zu verschicken, die hierzu ihre Einwilligung erteilt haben (siehe Art. 7 DSGVO). Die Zustimmung des Empfängers muss dokumentiert vorliegen und 40A auf Verlangen ausgehändigt werden. Diese Einwilligung muss insbesondere folgende Voraussetzungen erfüllen:
 - a. Die Einwilligung muss aktiv und gesondert erfolgen. Der Adressat muss entweder ein Kästchen anklicken/ankreuzen oder eine vergleichbar eindeutige Erklärung seiner Zustimmung abgeben. Diese Erklärung darf sich nur auf Werbung beziehen und nicht Bestandteil anderer Erklärungen (zum Beispiel Einwilligung in allgemeine Geschäftsbedingungen oder allgemeine Datenschutzbestimmungen) sein.
 - b. Die Einwilligung muss für den konkreten Fall und in informierter Weise abgegeben worden sein. Der Begünstigte der Einwilligung muss konkret benannt sein. Auch die Branchen und Bereiche, für die geworben werden soll, müssen klar und verständlich angegeben sein.
 - c. Eine Einwilligung Minderjähriger ist nur wirksam, wenn das 16. Lebensjahr vollendet ist oder wenn die Erziehungsberechtigten eingewilligt haben.
 - d. Beim Einholen der Einwilligung ist klar und deutlich darauf hinzuweisen, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Der Hinweis muss Informationen dazu enthalten, wie und gegenüber wem der Widerruf erfolgen kann. Die Möglichkeit des Widerrufs darf nicht komplizierter als das Erteilen der Einwilligung sein. Der erfolgte Widerruf muss nach spätestens fünf Werktagen umgesetzt sein.
- (2) Ausnahmsweise können auch ohne ausdrückliches Opt-in (siehe 2.1.) unter folgenden Voraussetzungen E-Mails an Kunden versendet werden:
 - a. bestehende Kundenbeziehung (Vorliegen eines entgeltlichen Austauschvertrags),
 - b. Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen,
 - c. Hinweis auf die jederzeitige Widerspruchsmöglichkeit (bei Erhebung und jeder Verwendung der E-Mail-Adresse), ohne dass hierfür andere als Übermittlungskosten nach den Basistarifen entstehen, und
 - d. kein Widerspruch erfolgt.
- (3) Beim Verwenden von E-Mail-Adressen, die der Anwender beziehungsweise seine Kunden von Dritten erworben haben, gilt:
 - a. Der Anwender beziehungsweise sein Kunde muss sich vor der Vornahme von Werbemaßnahmen vergewissern, dass eine Einwilligung (siehe Ziffer 2.2) vorliegt. Diese Einwilligung muss sich explizit auch auf den Anwender beziehungsweise seinen Kunden beziehen.
 - b. Bei der Datenerhebung muss für den Empfänger die Kenntnisnahme der Liste der begünstigten Unternehmen leicht und eindeutig möglich gewesen sein.
 - c. Die Anzahl der Unternehmen beziehungsweise Personen, für die die Adressdaten erhoben worden sind, war auf ein Maß reduziert, das das Weiterleiten der Nutzerdaten an einen unverhältnismäßig großen Kreis Dritter ausschließt. Die Anzahl muss dem Nutzer erlauben, die Tragweite und den Umfang seiner Einwilligung einfach zu erfassen sowie den rechtmäßigen Umgang mit seinen Daten einfach zu kontrollieren
 - d. Klarstellend sei darauf hingewiesen, dass die Unternehmen, für die die Adressdaten generiert werden, diese Adressdaten nicht an Dritte weitergeben dürfen, ohne dass vom Nutzer dafür gesondert eine weitere Einwilligung eingeholt wurde.
- (4) Der Anwender hat auf Aufforderung von 40A darzulegen, auf welche Weise die E-Mail-Adressen von Empfängern gesammelt worden sind.
- (5) Der Versand von Spam-E-mails ist nicht gestattet.
- (6) 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, von 40A auf eine Sperrliste gesetzt und von künftigen Zustellversuchen ausgeschlossen werden. Das gleiche gilt für die E-Mail-Adressen von Empfängern, von denen Beschwerden vorliegen.

3. E-Mail Anforderungen

- (1) In jeder versendeten geschäftsmäßigen E-Mail muss ein leicht erkennbares Impressum als Volltext enthalten sein. Das Impressum muss die nachfolgenden Angaben enthalten:
 - a. den Namen und die Anschrift, unter der der Auftraggeber niedergelassen ist, bei juristischen Personen zusätzlich die Rechtsform, das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind und die entsprechende Registernummer,
 - b. Kontaktinformationen, mindestens jedoch eine gültige Telefonnummer oder ein elektronisches Kontaktformular, sowie eine E-Mail-Adresse und Impressum mit Namen und Firmennamen des Anwenders und vollständiger Kontaktinformation (siehe §5 Absatz 1 TMG),

- c. eine Umsatzsteueridentifikationsnummer oder eine Wirtschaftsidentifikationsnummer, sofern vorhanden.

Weitergehende Informationspflichten nach nationalen Gesetzen bleiben unberührt. In jeder E-Mail ist darauf hinzuweisen, dass die Zusendung weiterer E-Mails abbestellt werden kann (Opt-out). Das Abbestellen von E-Mails muss grundsätzlich durch den Empfänger ohne Kenntnis von Zugangsdaten (beispielsweise Login und Passwort) möglich sein.

In der Kopf- und Betreffzeile der E-Mail darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

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.

- (5) Für die Bereitstellung von Bildern, Dateianhängen sowie zur Erstellung von E-Mails und den Adressimport ist es dem Anwender möglich, Dateien auf die Server von 40A 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 40A zu laden, die

- a. Viren enthalten
- b. Gegen das Urheberrecht verstoßen
- c. Sonstige illegale, sittenwidrige oder die Dienstleistung gefährdende Inhalte.

- (6) 40A behält sich vor, die Inhalte von E-Mails, die durch die Software versendet worden sind oder versendet werden sollen, stichprobenartig zu überprüfen.

4. Verstöße

- (1) Anwender, die gegen eine oder mehrere Teilnahmeregeln verstoßen, können unverzüglich und ohne vorherige Anündigung temporär oder dauerhaft von der Nutzung der Dienstleistung ausgeschlossen werden.

- (2) Bei Vorliegen von Beschwerden ist 40A berechtigt, die Versendung weiterer E-Mails des Anwenders ohne vorherige Anündigung zu unterbinden und das Nutzerkonto ggf. kostenpflichtig nach eigenem Ermessen zu sperren.

- (3) Wird ein Anwender wegen Verstoßes gegen die Teilnahmebedingungen von der Nutzung der Dienstleistung ausgeschlossen, besteht kein Anspruch auf die Erstattung bereits bezahlter Gebühren.

- (4) Erfolgt nachweislich aufgrund des Versands eines Mailings durch den Anwender die Sperrung einer oder mehrerer IP-Adressen oder Domains von 40A bzw. die Aufnahme einer oder mehrere IP-Adressen oder Domains von 40A in sogenannten Blacklists, so ist 40A berechtigt, den aktuellen Stundensatz zur Beseitigung des Zustands in Rechnung zu stellen und ggf. Schadensersatz zu verlangen.

5. Datenspeicherung

- (1) 40A hat das Recht, bei jedem Versand eines E-Mails die IP-Adressen des Anwenders für die Dauer von üblicherweise einem Jahr zu speichern.

- (2) 40A 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 Abmeldungen.

- (3) Daten von Abmeldungen und Beschwerden (E-Mail-Adresse des Empfängers, Datum, IP, Nutzer ID) werden üblicherweise dauerhaft gespeichert, um den gesetzlichen Vorschriften der DSGVO (insbesondere Art. 7 3) zu genügen.

- (4) 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 40A unverzüglich davon in Kenntnis zu setzen, damit 40A die unbefugte Nutzung unterbinden kann.

- (5) Zu Zwecken der technischen Analyse und der Fehlerbehebung hat 40A das Recht, in die Daten des Anwenders Einblick zu nehmen, auch ohne den Anwender hiervon in Kenntnis zu setzen.

- (6) 40A 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.

Anhang B:

Auftragsverarbeitung gemäß Art. 28 AB. 3 DS-GVO

zwischen dem Kunden
(Auftraggeber)

gegenüber der

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

1. Gegenstand und Dauer des Auftrages

Der Gegenstand des Auftrages 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 Auftrages (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten, Kreis der Betroffenen

- (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 Auftrages 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) Der Kreis der Betroffenen bestimmt sich nach den vom Auftraggeber in das vertragsgegenständliche System geladenen Daten (insb. Empfänger der E-Mail Newsletter)

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 Auftrages. 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. Insofern 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, Daten-portabilität 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 Auftrages 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) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung (einschließlich der Pflichten bzgl. Kontrollrechte des Auftraggebers) dem Unterauftragnehmer zu übertragen.
- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (5) 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.
- (6) 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, 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-Grundsatz).
- (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 (einschließlich Verstöße gegen Weisungen) 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) Der Umfang des Weisungsrechts ergibt sich anfänglich aus Ziff. 1 bzw. der Leistungsvereinbarung und kann vom Auftraggeber danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). 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.

11. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

12. Sicherheit der Verarbeitung

Das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung richtet sich gemäß Ziff. 4 der Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO für den „News & Mail Service“ der 4OfficeAutomation GmbH (Anhang C).

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. Zutrittskontrolle

Um eine physische Sicherheit der Daten zu gewährleisten, werden Kundendaten und Backups grundsätzlich nur in den Rechenzentren professioneller Hosting Provider mit entsprechenden TOMs (wie beispielsweise 1&2 oder myLoc) gespeichert und verarbeitet. Eine Datenspeicherung in den Räumen des Anbieters findet nicht statt.

2. Zugangskontrolle

Zugangsberechtigungen sind so konfiguriert, dass Personen nur zu den Bereichen Zugang haben, wo sie diesen aufgrund ihrer Funktion benötigen.

Alle Systeme sind mindestens durch Benutzernamen/Passwort geschützt.

Da die datenverarbeitenden Systeme in Rechenzentren untergebracht sind, ist ein physikalischer Zugang nur den autorisierten Mitarbeitern im Rahmen der TOMs des Rechenzentrums möglich.

Ein Fernzugriff ist nur in authentisierter Form möglich, so dass Manipulationen bei einem erfolgreichen Login immer einem Mitarbeiter zugeordnet werden können.

3. Zugriffskontrolle

Anwender können nach Angabe von Benutzername und Passwort auf Daten zugreifen, die durch den Versand eines Mailings entstanden sind, insbesondere auf Versandprotokolle und Trackingdaten. Die gleichen Daten sind zu Zwecken der Qualitätssicherung und der Verfolgung von Missbrauch des Systems auch dafür berechtigten Mitarbeitern des Anbieters und des Kundendienstes zugänglich.

4. Eingabekontrolle und Auftragskontrolle

Personenbezogene Daten werden immer dann an das System übermittelt, wenn ein Anwender ein Mailing versenden möchte und hierfür die entsprechenden Daten auf den Server lädt.

Nur solche personenbezogenen Daten, die für den Versand und die Personalisierung eines Mailings absolut notwendig sind, werden vom System über eine durch SSL gesicherte Leitung an den für den Versand zuständigen Server übermittelt. Diese Übermittlung ist nur von einem berechtigten Anwender durch die Benutzung des dafür vorgesehenen Add-Ins und der dafür bereitstehenden Web-Oberfläche möglich.

Jede Eingabe wird durch Protokolle dokumentiert, die Protokolle werden für 30 Tage gespeichert. Versandprotokolldaten, die beim Versand eines Mailings anfallen, werden für maximal ein Jahr gespeichert und anschließend automatisch gelöscht.

5. Verfügbarkeitskontrolle und Datensicherung

Personenbezogene Daten werden nicht auf Dauer gespeichert, sondern nach maximal einem Jahr automatisch gelöscht. Von allen Daten werden tägliche Backups angefertigt, die auf Amazon S3 Buckets in Deutschland End-to-End verschlüsselt übertragen und gespeichert werden. Ein Antivirussystem ist vorhanden, das System wird regelmäßig vom Anbieter überwacht und gepflegt. Seitens des Hostinganbieters gibt es zusätzlich eine externe Firewall, ein RAID System und eine unterbrechungsfreie Stromversorgung.

6. Trennungskontrolle

Die Daten der Anwender werden in unterschiedlichen Bereichen gespeichert. Ein Anwender kann nur nach Eingabe von Benutzerdaten und Passwort oder durch das dafür vorgesehene Add-In auf seine Protokolldaten zugreifen.

Der „News & Mail Service“ ist ein eigenständiges System und hat keinerlei Verbindung zu anderen Diensten des Anbieters.

Stand: 27.08.2025

Anhang D

Liste der Unterauftragnehmer für News&Mail Service

No	Unterauftragnehmer	Leistung
1	GoDaddy Deutschland GmbH c/o WeWork Friesenplatz 4 50672 Köln Deutschland	Bereitstellung von Domainnamen
2	IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	Server Hosting, Datenspeicherung
3	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Server Hosting, Datenspeicherung
4	STRATO AG Otto-Ostrowski-Straße 7 10249 Berlin Deutschland	Server Hosting, Datenspeicherung
5	Amazon Web Services EMEA, SARL, 38, Avenue John F. Kennedy L-1855 Luxembourg Rechenzentrum Frankfurt am Main	Speicherung verschlüsselter Backup-Daten (AES-256 Verschlüsselung)

Stand 27.08.2025