Auftragsverarbeitungsvertrag inkl. TOMs

hookfree UG (haftungsbeschränkt) · Version 1.0 · Stand: 07.06.2026

Auftragsverarbeitungsvertrag einschließlich Technischer und Organisatorischer Maßnahmen

für die hookfree Phishing Engine

Version: 1.0

Stand: 07.06.2026

zwischen

Kunde / Auftraggeber

nachfolgend „Auftraggeber“ genannt

und

hookfree UG (haftungsbeschränkt)

Buscher Weg 15

41751 Viersen

vertreten durch den Geschäftsführer Thomas Wüsten

E-Mail: info@hookfree.de

nachfolgend „Auftragnehmer“ oder „hookfree“ genannt.

Präambel

Der Auftraggeber nutzt Leistungen der hookfree Phishing Engine zur Vorbereitung, Durchführung und Auswertung kontrollierter Phishing-Simulationen und Awareness-naher Sicherheitsmaßnahmen.

Im Rahmen dieser Leistungen kann hookfree personenbezogene Daten im Auftrag des Auftraggebers verarbeiten. Dieser Auftragsverarbeitungsvertrag regelt die Rechte und Pflichten der Parteien nach Art. 28 Datenschutz-Grundverordnung.

Dieser Vertrag ergänzt die Allgemeinen Geschäftsbedingungen, die Leistungsbeschreibung / Produktbedingungen und sonstige vertragliche Vereinbarungen zwischen den Parteien.

1. Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch hookfree im Auftrag des Auftraggebers im Zusammenhang mit der Nutzung der hookfree Phishing Engine.

1.2 Die Verarbeitung erfolgt insbesondere zur Einrichtung und Verwaltung des Kundenmandanten, Verwaltung von Benutzerkonten, Vorbereitung von Phishing-Simulationen, Verwaltung und Prüfung von Empfängerlisten, technischen Durchführung von Simulationen, Versand von Simulations-E-Mails, Verarbeitung von Versand-, Zustell- und Trackingereignissen, Bereitstellung von Testmails, Erstellung von Auswertungen und Berichten, technischen Absicherung und Protokollierung sowie Umsetzung von Lösch-, Sperr- und Aufbewahrungsregeln.

1.3 Die Dauer der Verarbeitung richtet sich nach der Laufzeit des zugrunde liegenden Vertrags, den gebuchten Leistungen, gesetzlichen Aufbewahrungspflichten und den vereinbarten Löschfristen.

1.4 Nach Beendigung des Hauptvertrags oder nach Wegfall des Verarbeitungszwecks werden personenbezogene Daten nach Maßgabe dieses Vertrags gelöscht, anonymisiert oder zurückgegeben, sofern keine gesetzlichen Aufbewahrungspflichten oder berechtigten Dokumentationspflichten entgegenstehen.

2. Art und Zweck der Verarbeitung

2.1 Die Verarbeitung dient der Durchführung kontrollierter Phishing-Simulationen und der Bereitstellung der damit verbundenen Plattformfunktionen.

2.2 Die Verarbeitung umfasst insbesondere Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Einschränken, Löschen, Anonymisieren, Pseudonymisieren und Protokollieren.

2.3 Die Verarbeitung erfolgt ausschließlich für die in diesem Vertrag, der Leistungsbeschreibung und dem Hauptvertrag beschriebenen Zwecke.

2.4 hookfree verarbeitet personenbezogene Daten nicht für eigene Zwecke, soweit keine eigene datenschutzrechtliche Verantwortlichkeit, gesetzliche Pflicht oder berechtigter Sicherheitszweck vorliegt.

3. Kategorien personenbezogener Daten

Je nach Nutzung der Plattform können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

3.1 Daten von Kundenansprechpartnern und Plattformnutzern: Vorname, Nachname, geschäftliche E-Mail-Adresse, Telefonnummer, Rolle oder Funktion, Organisationszuordnung, Benutzerrolle in der Plattform, Login- und Sicherheitsstatus, Zwei-Faktor-Authentifizierungsstatus, Aktivierungsstatus, Kommunikationsdaten, Support- und Workflow-Nachrichten sowie Audit-Log-Daten.

3.2 Unternehmens- und Vertragsdaten mit Personenbezug: Ansprechpartnerdaten, Rechnungs-E-Mail-Adresse, Admin-E-Mail-Adresse, Kundennummer, Bestell- und Buchungsdaten, Zahlungsstatus, Accountprüfstatus, Domainprüfstatus, Vertragsbestätigungen sowie Akzeptanz von Vertragsunterlagen mit Zeitstempel.

3.3 Empfänger- und Simulationsdaten: E-Mail-Adresse, Vorname, Nachname, Abteilung, Organisationseinheit, Gruppenzuordnung, Empfängerdomain, Zugehörigkeit zu Empfängerlisten, Zugehörigkeit zu Simulationen, Versandstatus, Zustellstatus, Bounce- oder Fehlerstatus und Testmailstatus.

3.4 Tracking- und Ereignisdaten: Kampagnenbezug, Empfängerbezug, Trackingtoken, Link-Klick-Ereignisse, Formularereignisse, Zeitpunkte von Ereignissen, pseudonymisierte oder gehashte technische Metadaten, Zustell- und Versandereignisse sowie Berichtsdaten.

3.5 Technische Sicherheits- und Protokolldaten: Benutzer-ID, Mandanten-ID, Session- und Zugriffsdaten, IP-bezogene Sicherheitsinformationen, User-Agent-bezogene Sicherheitsinformationen, Rate-Limit-Informationen, Sicherheitsereignisse, Audit-Log-Einträge sowie Fehler- und Systemereignisse.

4. Kategorien betroffener Personen

Die Verarbeitung kann insbesondere Beschäftigte des Auftraggebers, Mitarbeitende, Führungskräfte, Auszubildende, interne und externe Nutzer innerhalb des berechtigten Organisationsbereichs, technische oder organisatorische Ansprechpartner, Administratoren des Kunden, Operatoren oder sonstige Plattformnutzer, Empfänger von Phishing-Simulationen, Rechnungskontakte und Supportkontakte betreffen.

5. Rollen der Parteien

5.1 Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, soweit er über Zwecke und Mittel der Verarbeitung personenbezogener Daten im Rahmen seiner Organisation entscheidet.

5.2 hookfree ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, soweit hookfree personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

5.3 Der Auftraggeber ist insbesondere verantwortlich für die Rechtmäßigkeit der Verarbeitung, Auswahl der betroffenen Personen, Zulässigkeit der Empfängerlisten, interne datenschutzrechtliche Bewertung, Einbindung von Datenschutzbeauftragten, Personalvertretungen oder sonstigen Stellen, Information betroffener Personen, Festlegung von Reporting- und Auswertungsanforderungen sowie Weisungen an hookfree.

5.4 hookfree ist verantwortlich für die vertragsgemäße, sichere und weisungsgebundene Verarbeitung im Rahmen dieses Vertrags.

6. Weisungen des Auftraggebers

6.1 hookfree verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern hookfree nicht durch Unionsrecht oder nationales Recht zu einer Verarbeitung verpflichtet ist.

6.2 Weisungen ergeben sich insbesondere aus diesem Vertrag, dem Hauptvertrag, der Leistungsbeschreibung, den Plattformkonfigurationen, den vom Auftraggeber gewählten Einstellungen, den vom Auftraggeber übermittelten Empfängerlisten, den im Workflow erteilten Freigaben sowie schriftlichen oder textförmlichen Einzelweisungen.

6.3 Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

6.4 hookfree informiert den Auftraggeber unverzüglich, wenn hookfree der Ansicht ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

6.5 hookfree ist berechtigt, die Ausführung einer Weisung auszusetzen, wenn konkrete Anhaltspunkte bestehen, dass die Weisung rechtswidrig ist, Missbrauch ermöglicht oder Sicherheitsrisiken begründet.

7. Vertraulichkeit

7.1 hookfree stellt sicher, dass Personen, die mit der Verarbeitung personenbezogener Daten befasst sind, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.2 Die Vertraulichkeitspflicht gilt auch nach Beendigung der Tätigkeit fort.

7.3 Personenbezogene Daten dürfen nur solchen Personen zugänglich gemacht werden, die den Zugriff zur Erfüllung ihrer Aufgaben benötigen.

8. Technische und organisatorische Maßnahmen

8.1 hookfree trifft angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten.

8.2 Die zum Zeitpunkt des Vertragsschlusses geltenden Maßnahmen sind in Anlage 2 beschrieben.

8.3 hookfree darf technische und organisatorische Maßnahmen weiterentwickeln und anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

8.4 Wesentliche Änderungen, die das Schutzniveau erheblich beeinflussen, werden dem Auftraggeber in geeigneter Weise mitgeteilt.

9. Unterauftragsverarbeiter

9.1 hookfree darf Unterauftragsverarbeiter einsetzen, soweit dies zur Leistungserbringung erforderlich ist und die Anforderungen des Art. 28 DSGVO eingehalten werden.

9.2 hookfree stellt sicher, dass Unterauftragsverarbeiter vertraglich mindestens in dem Umfang zum Datenschutz verpflichtet werden, wie hookfree gegenüber dem Auftraggeber verpflichtet ist.

9.3 Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

9.4 hookfree informiert den Auftraggeber über geplante Änderungen bei Unterauftragsverarbeitern. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

9.5 Erfolgt kein Widerspruch innerhalb einer angemessenen Frist, gilt die Änderung als genehmigt, sofern hookfree den Auftraggeber auf diese Folge hingewiesen hat.

10. Unterstützung des Auftraggebers

10.1 hookfree unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung datenschutzrechtlicher Pflichten, insbesondere bei Betroffenenanfragen, Berichtigung oder Löschung personenbezogener Daten, Einschränkung der Verarbeitung, Datenübertragbarkeit, Datenschutz-Folgenabschätzungen, Konsultation von Aufsichtsbehörden und Meldung von Datenschutzverletzungen.

10.2 Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der hookfree zur Verfügung stehenden Informationen.

10.3 Soweit Unterstützungsleistungen über den vertraglich geschuldeten Standardumfang hinausgehen oder durch besondere Weisungen des Auftraggebers verursacht werden, kann hookfree den Aufwand nach vorheriger Abstimmung gesondert berechnen, sofern keine gesetzliche Pflicht zur unentgeltlichen Unterstützung besteht.

11. Betroffenenrechte

11.1 Wendet sich eine betroffene Person unmittelbar an hookfree und ist erkennbar, dass die Anfrage eine Verarbeitung im Auftrag des Auftraggebers betrifft, wird hookfree die Anfrage an den Auftraggeber weiterleiten oder mit diesem abstimmen.

11.2 hookfree beantwortet solche Anfragen nicht eigenständig inhaltlich, soweit der Auftraggeber hierfür Verantwortlicher ist, es sei denn, der Auftraggeber weist hookfree hierzu an oder eine gesetzliche Pflicht besteht.

11.3 hookfree unterstützt den Auftraggeber im Rahmen der technischen Möglichkeiten bei der Erfüllung berechtigter Betroffenenrechte.

12. Meldung von Datenschutzverletzungen

12.1 hookfree informiert den Auftraggeber unverzüglich, wenn hookfree eine Verletzung des Schutzes personenbezogener Daten feststellt, die Daten des Auftraggebers betrifft.

12.2 Die Meldung enthält, soweit verfügbar, Art der Verletzung, betroffene Datenkategorien, betroffene Personengruppen, ungefähre Anzahl betroffener Datensätze, wahrscheinliche Folgen, bereits ergriffene Maßnahmen, empfohlene Maßnahmen und Ansprechpartner für Rückfragen.

12.3 hookfree trifft unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

12.4 Die Bewertung, ob eine Meldung an eine Aufsichtsbehörde oder betroffene Personen erforderlich ist, obliegt grundsätzlich dem Auftraggeber, soweit dieser Verantwortlicher ist.

13. Löschung und Rückgabe von Daten

13.1 Nach Abschluss der vertraglich vereinbarten Leistungen, nach Beendigung des Hauptvertrags oder nach Wegfall des Verarbeitungszwecks löscht oder anonymisiert hookfree personenbezogene Daten nach den vereinbarten Löschfristen.

13.2 Soweit der Auftraggeber vor Vertragsende eine Löschung verlangt, setzt hookfree diese im Rahmen der technischen Möglichkeiten und gesetzlichen Vorgaben um.

13.3 Gesetzliche Aufbewahrungspflichten, Abrechnungsdaten, Nachweisdaten und Sicherheitsprotokolle bleiben unberührt, soweit hookfree zu deren Speicherung berechtigt oder verpflichtet ist.

13.4 Bei einmaligen Simulationen werden personenbezogene Simulations- und Empfängerdaten grundsätzlich nach 30 Tagen gelöscht oder anonymisiert, soweit keine abweichende Vereinbarung besteht.

13.5 Berichte und aggregierte Auswertungen können grundsätzlich bis zu einem Jahr gespeichert werden, sofern keine abweichende Vereinbarung besteht.

13.6 Bei wiederkehrenden Simulationen können Berichte und aggregierte Auswertungen während der Vertragslaufzeit gespeichert werden und grundsätzlich ein Jahr nach Vertragsende gelöscht werden, sofern keine abweichende Vereinbarung besteht.

13.7 Personenbezogene Rohdaten, die für die weitere Leistungserbringung nicht mehr erforderlich sind, werden gelöscht, anonymisiert oder pseudonymisiert.

13.8 Backups werden nach dem jeweiligen Backup- und Löschzyklus überschrieben oder gelöscht. Eine gezielte Einzelöschung aus bereits bestehenden Backups kann technisch ausgeschlossen sein. In diesem Fall wird sichergestellt, dass gelöschte Daten bei einer Wiederherstellung nicht wieder produktiv genutzt oder erneut verarbeitet werden, soweit dies technisch und organisatorisch möglich ist.

14. Kontrollrechte und Nachweise

14.1 hookfree stellt dem Auftraggeber auf Anfrage geeignete Nachweise zur Einhaltung der Pflichten aus diesem Vertrag zur Verfügung.

14.2 Geeignete Nachweise können insbesondere Beschreibung der technischen und organisatorischen Maßnahmen, Sicherheits- und Datenschutzkonzepte, Zertifikate oder Prüfberichte, soweit vorhanden, Auskünfte zu Unterauftragsverarbeitern, Dokumentation relevanter Prozesse sowie Audit- oder Protokollauszüge in angemessenem Umfang sein.

14.3 Vor-Ort-Kontrollen sind nur nach vorheriger Abstimmung, mit angemessener Frist, zu üblichen Geschäftszeiten und unter Wahrung von Sicherheits- und Geheimhaltungsinteressen zulässig.

14.4 Kontrollen dürfen den Betrieb von hookfree nicht unverhältnismäßig beeinträchtigen und dürfen keine Daten anderer Kunden offenlegen.

14.5 Soweit eine Kontrolle über den üblichen Nachweisumfang hinausgeht, kann hookfree den entstehenden Aufwand nach vorheriger Abstimmung angemessen berechnen.

15. Internationale Datenübermittlung

15.1 Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die datenschutzrechtlichen Voraussetzungen erfüllt sind.

15.2 Soweit Drittlandübermittlungen erforderlich werden, setzt hookfree geeignete Garantien ein, insbesondere Angemessenheitsbeschlüsse, Standardvertragsklauseln oder andere gesetzlich zulässige Mechanismen.

15.3 Einzelheiten können sich aus der Liste der Unterauftragsverarbeiter ergeben.

16. Abgrenzung eigener Verantwortlichkeit von hookfree

16.1 Für bestimmte Verarbeitungsvorgänge kann hookfree eigenständig Verantwortlicher sein. Dies betrifft insbesondere eigene Website, eigene Interessenten- und Kundenkommunikation, Vertrags- und Rechnungsverwaltung, eigene Buchhaltung, eigene Sicherheits- und Missbrauchsprotokolle, eigene Systemadministration sowie rechtliche Nachweispflichten.

16.2 Diese Verarbeitungen werden in den Datenschutzhinweisen von hookfree beschrieben und sind nicht Gegenstand dieses Auftragsverarbeitungsvertrags, soweit hookfree insoweit nicht im Auftrag des Kunden handelt.

17. Pflichten des Auftraggebers

17.1 Der Auftraggeber ist für die Zulässigkeit der Verarbeitung personenbezogener Daten verantwortlich.

17.2 Der Auftraggeber stellt insbesondere sicher, dass Empfängerlisten rechtmäßig verwendet werden dürfen, Simulationen nur im eigenen berechtigten Organisationsbereich stattfinden, erforderliche interne Freigaben vorliegen, datenschutzrechtliche Informationspflichten erfüllt werden, erforderliche Beteiligungen von Datenschutzbeauftragten, Personalvertretungen oder sonstigen Stellen erfolgen, die gewählten Reporting-Einstellungen zulässig sind, personenbezogene Detailauswertungen nur genutzt werden, wenn hierfür eine Rechtsgrundlage besteht, und keine unzulässigen Inhalte oder Empfängerdaten übermittelt werden.

17.3 Der Auftraggeber informiert hookfree unverzüglich, wenn besondere Anforderungen, Einschränkungen oder Risiken bestehen.

18. Schlussbestimmungen

18.1 Änderungen und Ergänzungen dieses Vertrags bedürfen mindestens der Textform.

18.2 Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

18.3 Es gilt deutsches Recht.

18.4 Soweit dieser Vertrag keine abweichende Regelung enthält, gelten ergänzend die Regelungen des Hauptvertrags und der Allgemeinen Geschäftsbedingungen.

Anlage 1 – Beschreibung der Verarbeitung

1. Verfahren / Plattform

hookfree Phishing Engine.

2. Zweck der Verarbeitung

Bereitstellung einer SaaS-Plattform zur Vorbereitung, Durchführung, Verwaltung und Auswertung kontrollierter Phishing-Simulationen und Awareness-naher Sicherheitsmaßnahmen.

3. Leistungsbereiche

Registrierung und Mandantenverwaltung, Benutzer- und Rollenverwaltung, Account- und Domainprüfung, Empfängerlistenverwaltung, Vorlagenkatalog, Managed-Auftragsworkflow, technische Kampagnenplanung, Versand von Simulations-E-Mails, Testmailversand, Tracking von Ereignissen, Landingpage- und Redirect-Verarbeitung, Reporting und PDF-Berichte, Audit-Logging, Löschung, Anonymisierung und Retention.

4. Datenarten

Stammdaten von Ansprechpartnern, Benutzer- und Zugangsdaten, Kontaktdaten, Unternehmens- und Vertragsdaten, Empfängerdaten, Simulationsdaten, Versanddaten, Zustellstatus, Trackingereignisse, Formulareereignisse ohne Speicherung eingegebener Rohwerte, Reportingdaten, Audit- und Sicherheitsprotokolle.

5. Betroffene Personen

Beschäftigte des Auftraggebers, Mitarbeitende, Nutzer der Plattform, Administratoren, Ansprechpartner und Empfänger von Simulationen.

6. Standard-Löschfristen

Soweit nicht abweichend vereinbart: Personenbezogene Simulations- und Empfängerdaten bei einmaligen Simulationen grundsätzlich 30 Tage nach Abschluss der Simulation; Berichte bei einmaligen Simulationen grundsätzlich 1 Jahr; personenbezogene Simulations- und Empfängerdaten bei wiederkehrenden Simulationen grundsätzlich 30 Tage nach Abschluss der jeweiligen Simulation; Berichte bei wiederkehrenden Simulationen während der Vertragslaufzeit und grundsätzlich 1 Jahr nach Vertragsende; Testmail-Jobs und technische Kurzzeitdaten nach technischer Erforderlichkeit und Retention-Konzept; Audit-Logs nach Sicherheits-, Nachweis- und Aufbewahrungszweck; Vertrags- und Rechnungsdaten nach gesetzlichen Aufbewahrungspflichten.

7. Besonderheiten bei Formularsimulationen

Bei Formular- oder Login-Simulationen werden eingegebene Rohwerte nicht als Klarwerte gespeichert. Zulässig sind Statusinformationen wie Formular wurde abgesendet, E-Mail-Feld wurde befüllt, Passwortfeld wurde befüllt und Ereigniszeitpunkt. Nicht gespeichert werden konkret eingegebene E-Mail-Adressen im Formularfeld, konkret eingegebene Passwörter, konkrete Zugangscodes, konkrete Zahlungsdaten oder sonstige Freitext-Rohwerte aus Formularen.

Anlage 2 – Technische und Organisatorische Maßnahmen

1. Vertraulichkeit

hookfree setzt Zugriffskontrollen, individuelle Benutzerkonten, Passwortschutz, Zwei-Faktor-Authentifizierung, rollenbasierte Zugriffskontrolle, Trennung von Plattformrollen und Kundenrollen, Mandantentrennung, Zugriff nur nach Erforderlichkeit, administrative Zugriffe nur für berechtigte Personen, keine Anzeige von SMTP-Secrets oder technischen Geheimnissen im Frontend, sichere Speicherung von Zugangsdaten und Secrets sowie Einschränkung sensibler Administrationsbereiche ein.

2. Mandantentrennung

Die Plattform ist mandantenfähig aufgebaut. Maßnahmen sind tenantbezogene Datenmodelle, serverseitige Prüfung von Mandantenzugriffen, keine alleinige Sicherheitsentscheidung im Frontend, Backend als Sicherheitsinstanz, BFF-Prinzip zwischen Browser und Backend, serverseitige Verhinderung von Cross-Tenant-Zugriffen, fachliche und technische Trennung von Self-Managed- und Managed-Strukturen sowie keine Sichtbarkeit fremder Kundendaten.

3. Verschlüsselung und Transport

Maßnahmen sind TLS-Verschlüsselung für Webzugriffe, HTTPS für Plattform und relevante öffentliche Endpunkte, verschlüsselte Übertragung von Zugangsdaten, Schutz von Authentifizierungs-Cookies, sichere Token- und Session-Verarbeitung und keine Ausgabe sensibler Tokens an unberechtigte Nutzer.

4. Integrität

Maßnahmen sind Validierung von Eingaben, serverseitige Prüfung von Domains, Empfängerlisten, zulässigen Empfängerdomains, Rollen und Berechtigungen, Vertrags- und Accountstatus, Paket- und Kontingentgrenzen, Schutz vor unzulässigen Uploadgrößen, CSV-Importbeschränkungen, Plausibilitätsprüfungen im Managed-Workflow, Audit-Logs für sicherheitsrelevante Aktionen und Schutz vor Manipulation.

5. Verfügbarkeit und Belastbarkeit

Maßnahmen sind containerisierter Betrieb, Trennung von Frontend, Backend, Datenbank, Redis und Worker, Worker-basierte Verarbeitung von Versandjobs, Healthchecks, kontrollierte Deployments, Logprüfung nach Änderungen, Backup-Konzept, Wiederherstellungsplanung und technische Überwachung nach Betriebsstand.

6. Backup und Wiederherstellung

Die produktiven Systeme, insbesondere Engine, Mailcow, Mailinfrastruktur und zugehörige Daten, werden bei IONOS betrieben. Backups werden über die von IONOS bereitgestellte bzw. vermittelte Acronis-Backup-Lösung gesichert. Maßnahmen sind regelmäßige Backups relevanter Daten und Konfigurationen, Sicherung von Datenbankdaten, Sicherung relevanter Konfigurationsdaten, Sicherung von Plattformassets, Schutz von Backups vor unberechtigtem Zugriff und Wiederherstellungsprozesse nach technischem Konzept.

7. Schutz vor Überlastung und Missbrauch

Maßnahmen sind Rate-Limits für sicherheitsrelevante Endpunkte, Schutz von Login- und Passwort-Reset-Funktionen, Upload- und Bodygrößenlimits, Begrenzung von CSV-Importen, Versand- und Kampagnenlimits, Schutz öffentlicher Tracking-Endpunkte, technische Prüfung von Trackingdomains, Missbrauchserkennung und Sperrmöglichkeiten.

8. Datenschutzfreundliche Voreinstellungen

Maßnahmen sind datenschutzfreundliche Standardauswertungen, aggregierte Reports, Mindestgrößen für Abteilungs- und Gruppenauswertungen, personenbezogene Klickdetails nur bei bewusster Freischaltung, Reporting-Einstellungen je Mandant, serverseitige Anwendung der Datenschutzregeln und keine Berechnung verbotener Rohdaten im Kundenfrontend.

9. Formularschutz und Datenminimierung

Maßnahmen sind keine Speicherung eingegebener Passwort-Rohwerte, keine Speicherung konkreter Formular-Rohwerte bei Login-Simulationen, Speicherung nur notwendiger Statusinformationen, Sanitizing von Formularereignissen, neutrale Fehler- oder Folgeseiten nach Simulationseingaben, Begrenzung technischer Metadaten, Pseudonymisierung oder Hashing technischer Informationen, Lösch- und Retention-Prozesse sowie keine unnötige Anzeige personenbezogener Details.

10. Verfahren zur regelmäßigen Überprüfung

hookfree überprüft und verbessert technische und organisatorische Maßnahmen regelmäßig oder anlassbezogen, insbesondere bei neuen Plattformfunktionen, Sicherheitsupdates, Änderungen der Infrastruktur, erkannten Schwachstellen, Datenschutzanforderungen, Kundenanforderungen, internen Audits oder technischen Zwischenfällen.

Anlage 3 – Unterauftragsverarbeiter

1. Hosting / Serverinfrastruktur

Dienstleister: IONOS SE bzw. mit IONOS verbundene Hosting- und Infrastrukturdienstleister.

Zweck: Serverbetrieb, Hosting, Netzwerk, Infrastruktur, Betrieb der Engine, Betrieb der Mailserver-/Mailcow-Infrastruktur und technischer Plattformbetrieb.

Datenkategorien: Plattformdaten, Datenbankdaten, technische Daten, Maildaten, Konfigurationsdaten und Backups.

Ort der Verarbeitung: grundsätzlich Deutschland / EU, abhängig vom konkret gebuchten Produkt.

Hinweis: Die relevanten Systeme von hookfree, insbesondere hookfree Phishing Engine, Mailcow, Mailinfrastruktur und zugehörige Serverdienste, werden bei IONOS betrieben.

2. Backup-Dienstleister

Dienstleister: Acronis über IONOS bzw. durch IONOS bereitgestellte Acronis-Backup-Lösung.

Zweck: Datensicherung, Wiederherstellung, Betriebssicherheit und Schutz vor Datenverlust.

Datenkategorien: Plattformdaten, Datenbankdaten, Maildaten, Konfigurationsdaten, Serverdaten und Backupdaten.

Ort der Verarbeitung: abhängig von der durch IONOS bereitgestellten Backup-Infrastruktur.

Hinweis: Backups der hookfree-Systeme werden über den IONOS/Acronis-Backupdienst gesichert.

3. Zahlungsabwicklung

Dienstleister: Stripe Payments Europe, Ltd. bzw. Stripe-Unternehmen.

Zweck: Zahlungsabwicklung, Checkout, Zahlungsstatus, Rechnungs- und Zahlungsinformationen.

Datenkategorien: Zahlungsdaten, Kontaktdaten, Rechnungsdaten, Checkout- und Zahlungsstatus.

Ort der Verarbeitung: EU und ggf. Drittländer nach Stripe-Datenschutzregelungen.

Hinweis: Vollständige Zahlungsdaten wie vollständige Kreditkartennummern werden nicht durch hookfree gespeichert.

4. Steuerberatung / Buchhaltung

Dienstleister: Steuerberater, Buchhaltungs- oder Rechnungsdienstleister.

Zweck: Buchhaltung, Rechnungswesen, steuerliche Pflichten.

Datenkategorien: Rechnungsdaten, Kundendaten, Zahlungsdaten.

Hinweis: Diese Verarbeitung betrifft in der Regel eigene Verantwortlichkeit oder gesetzliche Pflichten von hookfree und nicht zwingend Auftragsverarbeitung für Simulationsdaten.

Anlage 4 – Weisungs- und Kontaktwege

Standardweisungen erfolgen über Plattformfunktionen, gewählte Einstellungen, Empfängerlisten, Workflow-Freigaben, Testmail-Anforderungen, verbindliche Beauftragung, Supportanfragen und E-Mail-Kommunikation.

Datenschutzrelevante Einzelweisungen können in Textform an hookfree übermittelt werden: info@hookfree.de.

Anlage 5 – Besondere Regelungen für Phishing-Simulationen

1. hookfree speichert im Rahmen von Simulationen keine eingegebenen echten Passwörter im Klartext.

2. Simulationen dürfen nicht dazu genutzt werden, echte Zugangsdaten, Zahlungsdaten, Ausweisdaten, Gesundheitsdaten oder vergleichbare sensible Rohdaten zu erheben.

3. Die Auswertung beschränkt sich grundsätzlich auf Ereignisse und Statusinformationen, beispielsweise E-Mail versendet, Zustellung fehlgeschlagen, Link geklickt, Formular abgesendet, E-Mail-Feld befüllt oder Passwortfeld befüllt.

4. Der Auftraggeber entscheidet über Empfängerkreis, interne Nutzung der Ergebnisse, Reporting-Freigaben und organisatorische Maßnahmen.

5. Soweit nicht anders konfiguriert, werden Auswertungen aggregiert und datenschutzfreundlich dargestellt. Personenbezogene Detailansichten werden nur bewusst und nach entsprechender Freischaltung bereitgestellt.