

Auftragsverarbeitungsvertrag

einschließlich Technischer und Organisatorischer Maßnahmen
für die E-Learning-Plattform hookfree Academy

Version: 1.0 · Stand: 14.04.2026

<p>Auftraggeber Kunde / Auftraggeber</p> <p>nachfolgend „Auftraggeber“ genannt</p>	<p>Auftragnehmer hookfree UG (haftungsbeschränkt) Buscher Weg 15 41751 Viersen vertreten durch den Geschäftsführer Thomas Wüsten E-Mail: info@hookfree.de</p> <p>nachfolgend „Auftragnehmer“ oder „hookfree“ genannt</p>
----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Präambel

Der Auftraggeber nutzt die E-Learning-Plattform hookfree Academy zur Bereitstellung, Verwaltung, Durchführung und Auswertung von Online-Schulungen, insbesondere zur Verwaltung von Mitarbeitenden, Zuweisung von Kursen, Erfassung von Lernfortschritten, Durchführung von Tests, Bereitstellung von Zertifikaten, Reporting, Lizenzverwaltung sowie für Benachrichtigungen und Erinnerungen im Zusammenhang mit Schulungsmaßnahmen.

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 E-Learning-Plattform hookfree Academy.

1.2 Die Verarbeitung erfolgt insbesondere zur Einrichtung und Verwaltung des Kundenmandanten, Verwaltung von Benutzerkonten, Rollen und Berechtigungen, Abbildung von Organisationen und Abteilungen, Bereitstellung und Zuweisung von Kursen, Erfassung von Lernfortschritten, Verarbeitung von SCORM- und Video-Fortschrittsdaten, Durchführung und Bewertung von Tests, Ausstellung und Bereitstellung von Zertifikaten, Erstellung von Auswertungen und Reports, Lizenzverwaltung, Versand von System-, Kurs-, Erinnerungs- und Benachrichtigungsmails, Support- und Ticketbearbeitung, technischen Absicherung, 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, berechtigten Nachweisinteressen, offenen Nachforderungen, Abrechnungsfragen oder sonstigen berechtigten Dokumentationspflichten entgegenstehen.

2. Art und Zweck der Verarbeitung

2.1 Die Verarbeitung dient der Bereitstellung einer mandantenfähigen E-Learning-Plattform zur Verwaltung von Mitarbeitenden, Bereitstellung und Zuweisung von Kursen, Erfassung von Lernfortschritten, Durchführung von Tests, Ausstellung von Zertifikaten, Reporting, Lizenzverwaltung sowie Versand von Kursbenachrichtigungen, Erinnerungen und Admin-Zusammenfassungen.

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, berechtigter Sicherheitszweck oder berechtigter Nachweiszweck 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, Abteilungszuordnung, Benutzerrolle in der Plattform, Login- und Sicherheitsstatus, Zwei-Faktor-Authentifizierungsstatus, Aktivierungsstatus, Kommunikationsdaten, Support- und Ticketdaten sowie Audit-Log-Daten.

3.2 Organisations- und Vertragsdaten mit Personenbezug: Ansprechpartnerdaten, Rechnungs-E-Mail-Adresse, Admin-E-Mail-Adresse, Kundennummer, Angebots-, Vertrags- und Rechnungsdaten, Lizenzdaten, gebuchte Lizenzanzahl, Lizenzverlauf, Nachlizenzierungsdaten, Vertragsbestätigungen sowie Akzeptanz von Vertragsunterlagen mit Zeitstempel.

3.3 Kurs- und Zuweisungsdaten: Kurszuweisungen, Pflichtkursstatus, Abteilungs- und Mitarbeiterzuweisungen, Sichtbarkeit von Kursen, Kursstatus, Kursbeginn, Kursfortschritt, Abschlussstatus, Kurs-Reset-Informationen und organisatorische Zuordnungen.

3.4 Lernfortschritts- und Testdaten: SCORM-Fortschrittsdaten, Video-Fortschrittsdaten, Lernstatus, Bearbeitungsstand, Zeitpunkte von Start, Fortschritt und Abschluss, Teststatus, Testergebnisse, Punktzahl, bestanden oder nicht bestanden, Testfreigaben und technische Lernstatusdaten.

3.5 Zertifikatsdaten: Name, Kurs, Abschlussdatum, Zertifikatsstatus, Zertifikats-ID, Zertifikatsdatei, Downloadinformationen, technische Nachweisdaten sowie Historie bereits erzeugter Schulungsnachweise.

3.6 Reporting- und Auswertungsdaten: aggregierte und gegebenenfalls personenbezogene Auswertungen zu Kurszuweisungen, Lernfortschritten, Abschlüssen, Zertifikaten, Pflichtkursen, Lizenzständen, Lizenzverläufen und organisationsbezogenen Schulungskennzahlen.

3.7 Benachrichtigungs- und Maildaten: Systemmails, Aktivierungsmails, Passwort-Reset-Mails, Kursbenachrichtigungen, Erinnerungsmails, Admin-Zusammenfassungen, Ticketbenachrichtigungen, Sicherheitsmeldungen, Versandstatus, Zustellstatus, Fehlerstatus, Zeitpunkte und Mail-Logs.

3.8 Support- und Ticketdaten: Ticketinhalte, Nachrichten, interne Notizen, Anhänge, Bearbeitungsstatus, zuständige Personen, Kommunikationsverlauf und technische Supportinformationen.

3.9 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, Administratoren, operative Verwaltungsrollen, Reportingrollen, Lernende, technische oder organisatorische Ansprechpartner, Rechnungskontakte, Supportkontakte und sonstige vom Auftraggeber in der Plattform angelegte oder verwaltete Nutzer betreffen.

5. Besondere Kategorien personenbezogener Daten

5.1 Die Plattform ist grundsätzlich nicht darauf ausgelegt, besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO zu verarbeiten.

5.2 Der Auftraggeber darf keine besonderen Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, Religionsdaten, Gewerkschaftsdaten, Daten zur sexuellen Orientierung, biometrische Daten, genetische Daten oder vergleichbare sensible Daten in Nutzerfeldern, Kursinhalten, Freitexten, Tickets, Uploads, SCORM-Paketen, Videos oder sonstigen Plattformbereichen hinterlegen, sofern dies nicht ausdrücklich vereinbart wurde.

5.3 Stellt der Auftraggeber dennoch solche Daten bereit, ist er für die Zulässigkeit, Rechtsgrundlage und etwaige besondere Schutzmaßnahmen verantwortlich. hookfree ist berechtigt, die Verarbeitung solcher Daten abzulehnen, Inhalte zu sperren oder die Löschung zu verlangen, soweit keine ausdrückliche Vereinbarung besteht.

6. Rollen der Parteien

6.1 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.

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

6.3 Der Auftraggeber ist insbesondere verantwortlich für die Rechtmäßigkeit der Verarbeitung, Auswahl der betroffenen Personen, Anlage und Verwaltung von Nutzerkonten, Zuweisung von Kursen, Einstufung von Pflichtkursen, Zulässigkeit von Lernfortschritts- und Zertifikatsverarbeitung, interne datenschutzrechtliche Bewertung, Einbindung von Datenschutzbeauftragten, Personalvertretungen oder sonstigen Stellen, Information betroffener Personen, Festlegung von Reporting- und Auswertungsanforderungen sowie Weisungen an hookfree.

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

7. Weisungen des Auftraggebers

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

7.2 Weisungen ergeben sich insbesondere aus diesem Vertrag, dem Hauptvertrag, der Leistungsbeschreibung, den Plattformkonfigurationen, den vom Auftraggeber gewählten Einstellungen, Nutzer- und Kursverwaltungen, Kurszuweisungen, Rollenvergaben, Benachrichtigungseinstellungen, Supportanfragen sowie schriftlichen oder textförmlichen Einzelweisungen.

7.3 Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

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

7.5 hookfree ist berechtigt, die Ausführung einer Weisung auszusetzen, wenn konkrete Anhaltspunkte bestehen, dass die Weisung rechtswidrig ist, Missbrauch ermöglicht, Sicherheitsrisiken begründet oder Rechte betroffener Personen oder Dritter verletzt.

8. Vertraulichkeit

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

8.2 Die Vertraulichkeitspflicht gilt auch nach Beendigung der Tätigkeit fort.

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

9. Technische und organisatorische Maßnahmen

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

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

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

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

10. Unterauftragsverarbeiter

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

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

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

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

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

11. Unterstützung des Auftraggebers

11.1 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.

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

11.3 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.

12. Betroffenenrechte

12.1 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.

12.2 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.

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

13. Meldung von Datenschutzverletzungen

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

13.2 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.

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

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

14. Löschung und Rückgabe von Daten

14.1 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.

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

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

14.4 Nutzerkonten, Kurszuweisungen, Lernfortschritte, Zertifikate, Reports, Lizenzdaten, Benachrichtigungseinstellungen und zugehörige Nachweisdaten werden während der Vertragslaufzeit gespeichert, soweit sie für die Leistungserbringung, Dokumentation oder Nachvollziehbarkeit erforderlich sind.

14.5 Bereits erzeugte Zertifikate und Schulungsnachweise bleiben als historische Nachweise erhalten. Dies gilt auch, wenn ein Kurs zurückgesetzt oder erneut bearbeitet wird.

14.6 Nach Vertragsende werden personenbezogene Plattformdaten grundsätzlich innerhalb von 90 Tagen gelöscht oder anonymisiert, sofern keine offenen Nachforderungen, Abrechnungsfragen, gesetzlichen Aufbewahrungspflichten, berechtigten Nachweisinteressen oder abweichenden Vereinbarungen entgegenstehen.

14.7 Kundeneigene Kursinhalte, Dateien, SCORM-Pakete, Videos und Materialien werden nach Vertragsende nach Maßgabe der Vereinbarung gelöscht, zurückgegeben oder anonymisiert, sofern keine berechtigten Gründe für eine weitere Speicherung bestehen.

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

14.9 Backups werden nach dem jeweiligen Backup- und Löschzyklus überschrieben oder gelöscht. Eine gezielte Einzel Löschung 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.

15. Kontrollrechte und Nachweise

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

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

15.3 Kontrollen erfolgen vorrangig durch geeignete Dokumentationen, Auskünfte, Nachweise, strukturierte Fragenkataloge oder sonstige angemessene Remote-Verfahren.

15.4 Weitergehende Kontrollen sind nur nach vorheriger Abstimmung, mit angemessener Frist, zu üblichen Geschäftszeiten und unter Wahrung von Sicherheits-, Geheimhaltungs- und Betriebsinteressen zulässig.

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

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

16. Internationale Datenübermittlung

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

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

16.3 Einzelheiten können sich aus der Liste der Unterauftragsverarbeiter ergeben.

17. Abgrenzung eigener Verantwortlichkeit von hookfree

17.1 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.

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

17.3 Steuerberatungs-, Buchhaltungs- oder Rechnungsverarbeitungen betreffen regelmäßig die eigene Verantwortlichkeit oder gesetzliche Pflichten von hookfree und sind nicht Bestandteil der Auftragsverarbeitung für Plattform-, Lern- oder Kursdaten des Auftraggebers.

18. Pflichten des Auftraggebers

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

18.2 Der Auftraggeber stellt insbesondere sicher, dass Nutzerkonten rechtmäßig angelegt werden dürfen, Kurszuweisungen und Pflichtkurs-Einstufungen zulässig sind, 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 personenbezogenen Daten übermittelt werden.

18.3 Der Auftraggeber ist für die Rechtmäßigkeit der von ihm bereitgestellten Kursinhalte, SCORM-Pakete, Videos, Texte, Dateien, Materialien, Freitexte und sonstigen Inhalte verantwortlich.

18.4 Der Auftraggeber stellt sicher, dass kundeneigene Kursinhalte keine unzulässigen personenbezogenen Daten, keine besonderen Kategorien personenbezogener Daten und keine rechtswidrigen Inhalte enthalten, sofern dies nicht ausdrücklich vereinbart wurde.

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

19. Schlussbestimmungen

19.1 Änderungen und Ergänzungen dieses Vertrags bedürfen mindestens der Textform.

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

19.3 Es gilt deutsches Recht.

19.4 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

E-Learning-Plattform hookfree Academy.

2. Zweck der Verarbeitung

Bereitstellung einer mandantenfähigen SaaS-Plattform zur Verwaltung von Mitarbeitenden, Bereitstellung und Zuweisung von Kursen, Erfassung von Lernfortschritten, Durchführung von Tests, Ausstellung von Zertifikaten, Reporting, Lizenzverwaltung sowie Versand von Kursbenachrichtigungen, Erinnerungen und Admin-Zusammenfassungen.

3. Leistungsbereiche

Mandantenverwaltung, Benutzer- und Rollenverwaltung, organisationsbezogene und abteilungsbezogene Verwaltung, Domainbeschränkung für Nutzeranlage, Kursverwaltung, Bereitstellung von Standardkursen, Einbindung kundeneigener SCORM- und Videokurse, Kurszuweisung, Pflichtkursverwaltung, Lernfortschrittserfassung, Testauswertung, Zertifikatsbereitstellung, Reporting und Exporte, Lizenzverwaltung und Lizenzverlauf, Benachrichtigungen, Erinnerungsmails, Admin-Zusammenfassungen, Ticket- und Supportfunktionen, Audit-Logging, Sicherheitslogging, Löschung, Anonymisierung und Retention.

4. Datenarten

Stammdaten von Ansprechpartnern, Benutzer- und Zugangsdaten, Kontaktdaten, Organisations- und Abteilungsdaten, Rollen und Berechtigungen, Kurszuweisungen, Lernfortschritte, SCORM- und Video-Fortschrittsdaten, Testdaten, Zertifikatsdaten, Reportingdaten, Lizenzdaten, Benachrichtigungsdaten, Mail-Logs, Ticketdaten, Audit- und Sicherheitsprotokolle sowie technische Zugriffsdaten.

5. Betroffene Personen

Beschäftigte des Auftraggebers, Mitarbeitende, Führungskräfte, Auszubildende, Nutzer der Plattform, Lernende, Administratoren, Manager, Reportingrollen, Ansprechpartner, Rechnungskontakte und Supportkontakte.

6. Standard-Löschfristen

Soweit nicht abweichend vereinbart: Nutzerkonten, Lernfortschritte, Zertifikate, Reports, Lizenzdaten und Nachweisdaten während der Vertragslaufzeit; nach Vertragsende grundsätzlich Löschung oder Anonymisierung personenbezogener Plattformdaten innerhalb von 90 Tagen, sofern keine offenen Nachforderungen, Abrechnungsfragen, gesetzlichen Aufbewahrungspflichten, berechtigten Nachweisinteressen oder abweichenden Vereinbarungen entgegenstehen; Vertrags- und Rechnungsdaten nach gesetzlichen Aufbewahrungspflichten; Sicherheits- und Audit-Logs nach Sicherheits-, Nachweis- und Aufbewahrungszweck; Backups nach Backup- und Löschzyklus.

7. Besonderheiten bei Zertifikaten und Kurs-Reset

Bereits erzeugte Zertifikate und Schulungsnachweise bleiben als historische Nachweise erhalten. Dies gilt auch dann, wenn ein Kurs zurückgesetzt wird oder Lernfortschrittsdaten für eine erneute Bearbeitung neu aufgebaut werden.

8. Besonderheiten bei kundeneigenen Kursinhalten

Kundeneigene Kursinhalte, SCORM-Pakete, Videos, Texte und Dateien werden ausschließlich zur Bereitstellung innerhalb des jeweiligen Kundenmandanten verarbeitet. Sie werden nicht für andere Kunden, eigene Schulungsprodukte, Werbezwecke oder sonstige Zwecke außerhalb der Vertragsdurchführung verwendet.

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 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 sowie keine Sichtbarkeit fremder Kundendaten.

3. Rollen- und Berechtigungskontrolle

Die Plattform nutzt ein rollenbasiertes Berechtigungsmodell. Rollen und Berechtigungen werden serverseitig geprüft. Kundenrollen, Plattformrollen, Supportrollen, Verwaltungsrollen, Reportingrollen und Lernendenrollen sind voneinander getrennt. Kritische Aktionen wie Benutzerverwaltung, Kursverwaltung, Reportingzugriff, Lizenzverwaltung, 2FA-Reset und administrative Einstellungen sind rollenabhängig beschränkt.

4. Domainbeschränkung bei Nutzeranlage

Das Hinzufügen neuer Mitarbeitender ist grundsätzlich auf die für die Organisation freigegebene E-Mail-Domain beschränkt. Weitere Organisationsdomains können nur nach Abstimmung mit dem Support und nach entsprechender Freigabe ergänzt werden. Dadurch wird das Risiko reduziert, versehentlich oder missbräuchlich Nutzer außerhalb des berechtigten Organisationsbereichs anzulegen.

5. 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.

6. Integrität

Maßnahmen sind Validierung von Eingaben, serverseitige Prüfung von Domains, Benutzerrollen, Mandantenzugriffen, Kurszuweisungen, Abteilungsfreigaben, Pflichtkurs-Einstellungen, Vertrags- und Accountstatus, Uploadgrößen, Dateiarten, Plausibilitätsprüfungen, Audit-Logs für sicherheitsrelevante Aktionen und Schutz vor Manipulation.

7. Verfügbarkeit und Belastbarkeit

Maßnahmen sind containerisierter Betrieb, Trennung von Frontend, Backend, Datenbank und weiteren technischen Komponenten, Healthchecks, kontrollierte Deployments, Logprüfung nach Änderungen, Backup-Konzept, Wiederherstellungsplanung und technische Überwachung nach Betriebsstand.

8. Backup und Wiederherstellung

Die produktiven Systeme, insbesondere hookfree Academy, Datenbank, 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 und Kursinhalten, Schutz von Backups vor unberechtigtem Zugriff und Wiederherstellungsprozesse nach technischem Konzept.

9. Schutz vor Überlastung und Missbrauch

Maßnahmen sind Rate-Limits für sicherheitsrelevante Endpunkte, Schutz von Login- und Passwort-Reset-Funktionen, Upload- und Bodygrößenlimits, Begrenzung von Importen, Schutz öffentlicher und interner Endpunkte, Missbrauchserkennung und Sperrmöglichkeiten.

10. Datenschutzfreundliche Voreinstellungen

Maßnahmen sind rollenbasierte Zugriffsbeschränkungen, mandantenbezogene Auswertungen, datenschutzfreundliche Reports, zweckgebundene Verarbeitung von Lernfortschritten und Zertifikaten, keine unnötige Anzeige personenbezogener Details, beschränkter Zugriff auf Reportingdaten sowie serverseitige Anwendung von Datenschutz- und Berechtigungsregeln.

11. Schutz von Kursinhalten und Uploads

Kursinhalte, SCORM-Pakete, Videodateien, Zertifikate und sonstige Plattforminhalte werden nach technischem Konzept geschützt bereitgestellt. Der Zugriff auf Lerninhalte erfolgt grundsätzlich nur für berechtigte Nutzer mit entsprechender Kurszuweisung oder Rolle. Uploads können durch Dateityp-, Größen- und Plausibilitätsprüfungen beschränkt werden.

12. Protokollierung und Nachvollziehbarkeit

Sicherheitsrelevante Aktionen werden durch Audit- und Sicherheitslogs nachvollziehbar gemacht. Dies umfasst insbesondere Login-Ereignisse, fehlgeschlagene Logins, 2FA-Ereignisse, administrative Änderungen, Rollen- und Nutzeränderungen, sicherheitsrelevante Systemereignisse und Supportvorgänge, soweit technisch vorgesehen.

13. 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 hookfree Academy, Betrieb der Datenbank, Betrieb der Mailserver-/Mailcow-Infrastruktur und technischer Plattformbetrieb.

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

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

Hinweis: Die relevanten Systeme von hookfree, insbesondere hookfree Academy, 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, Kursinhalte, Zertifikatsdaten 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. Mailinfrastruktur

Dienstleister / Betrieb: Von hookfree betriebene Mailcow-/Mailserver-Infrastruktur auf IONOS-Systemen.

Zweck: Versand von Systemmails, Aktivierungsmails, Passwort-Reset-Mails, Kursbenachrichtigungen, Erinnerungsmails, Admin-Zusammenfassungen, Ticketbenachrichtigungen, Sicherheitsmeldungen und sonstigen transaktionalen Plattformmails.

Datenkategorien: Empfängeradressen, Absenderdaten, Mailinhalte, technische Versanddaten, Zustell- und Fehlerstatus, Mail-Logs.

Ort der Verarbeitung: grundsätzlich Deutschland / EU, abhängig vom konkret genutzten IONOS-System.

Hinweis: Der Mailversand erfolgt über die von hookfree betriebene Mailinfrastruktur. Soweit hierfür IONOS-Infrastruktur genutzt wird, ist diese bereits dem Hosting- und Infrastrukturbereich zugeordnet.

Anlage 4 – Weisungs- und Kontaktwege

Standardweisungen erfolgen über Plattformfunktionen, gewählte Einstellungen, Benutzeranlage, Rollenvergabe, Kurszuweisungen, Pflichtkurs-Einstellungen, Benachrichtigungseinstellungen, Reporting-Einstellungen, Supportanfragen und E-Mail-Kommunikation.

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

Anlage 5 – Besondere Regelungen für E-Learning, Zertifikate und kundeneigene Kursinhalte

- 1. Lernfortschritte, Testdaten und Abschlussinformationen werden zur Durchführung, Steuerung, Auswertung und Dokumentation von Schulungsmaßnahmen verarbeitet.**
- 2. Zertifikate dienen als Schulungsnachweis und können als historische Nachweise erhalten bleiben. Dies gilt auch dann, wenn ein Kurs zurückgesetzt oder erneut bearbeitet wird.**
- 3. Kundeneigene Kursinhalte, SCORM-Pakete, Videos, Texte, Dateien und Materialien bleiben Inhalte des Auftraggebers. hookfree verwendet diese Inhalte nicht für andere Kunden, eigene Schulungsprodukte, Werbezwecke oder sonstige Zwecke außerhalb der Vertragsdurchführung.**
- 4. Der Auftraggeber bleibt verantwortlich für Rechtmäßigkeit, Inhalte, Rechtlklärung, Datenschutzkonformität und interne Freigabe der von ihm bereitgestellten Kursinhalte.**
- 5. Der Auftraggeber bleibt verantwortlich für die Auswahl der betroffenen Personen, Kurszuweisungen, Pflichtkurs-Einstufungen, Abteilungsfreigaben, interne Kommunikation, Rechtsgrundlagen, Beteiligung interner Stellen und Nutzung der Reports.**
- 6. Besondere Kategorien personenbezogener Daten dürfen nicht ohne ausdrückliche Vereinbarung in der Plattform verarbeitet werden.**
- 7. Das Hinzufügen neuer Mitarbeitender ist grundsätzlich auf die für die Organisation freigegebene E-Mail-Domain beschränkt. Weitere Organisationsdomains können nur nach Abstimmung und Freigabe durch hookfree ergänzt werden.**
- 8. Benachrichtigungen, Erinnerungsmails und Admin-Zusammenfassungen dienen der Unterstützung der Schulungsorganisation. Eine erfolgreiche Zustellung jeder einzelnen Nachricht wird nicht garantiert, da diese von Empfängersystemen, Mailservern, Spamfiltern, Sicherheitslösungen und sonstigen externen Faktoren abhängig sein kann.**

Unterzeichnung

Dieser Auftragsverarbeitungsvertrag einschließlich der Anlagen 1 bis 5 wird Bestandteil des Vertragsverhältnisses zwischen den Parteien.

Auftraggeber	Auftragnehmer
Ort, Datum: _____	Ort, Datum: _____
Name / Organisation: _____	Name: Thomas Wüsten
Name der unterzeichnenden Person: _____	Funktion: Geschäftsführer
Funktion: _____	Unterschrift: _____
Unterschrift: _____	