Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen dem lexoffice Kunden (Verantwortlicher) und der Haufe Service Center GmbH (Auftragsverarbeiter), Munzinger Straße 9, 79111 Freiburg wird nachfolgender Vertrag geschlossen (**Vertrag als PDF herunterladen**).

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung des in Ziffer 1 näher bezeichneten Softwaremoduls lexoffice (im Weiteren Lizenzvereinbarung) des Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit dem Dienstleistungsvertrag – eine Übertragung von ‚Funktionen' ist ausdrücklich nicht beabsichtigt.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

In den im Bestellprozess (Account-Registrierung) erworbenen lexoffice Versionen gehören dazu im Kern (1) die automatisierte Erstellung und Verbuchung von Ausgangsbelegen wie z.B. Angeboten, Rechnungen, Lieferscheinen etc., (2) die automatisierte Erfassung, Erkennung und Verbuchung von Eingangsbelegen, wie z.B. Kassenbelegen oder Lieferantenrechnungen, (3) der automatisierte Abgleich von Eingangs- und Ausgangsbelegen mit Zahlungsvorgängen angebundener Online-Bankkonten sowie (4) die automatisierte Erfassung und Speicherung von Kunden- und Lieferantendaten.

In den im Bestellprozess (Account-Registrierung) erworbenen lexoffice Versionen ist es zudem möglich über den „Kundenmanager" Dateien hochzuladen und mit Dritten zu teilen. Dabei trägt der Verantwortliche die volle Verantwortung für die hochgeladenen Dateien, deren Inhalt vom Auftragsverarbeiter nicht geprüft wird.

In der Version "Lohn & Gehalt" ist es zusätzlich möglich, Löhne und Gehälter von Beschäftigten zu erfassen, zu verbuchen und zu überweisen, sowie automatisiert die gesetzlich vorgeschriebenen Meldungen an die Sozialversicherungsträger und an das Finanzamt abzusetzen.

Der Gegenstand dieses Auftrags ergibt sich im Übrigen aus der bestehenden Lizenzvereinbarung, auf die hier verwiesen wird (im Weiteren „Lizenzvereinbarung"). Dabei handelt es sich um die Verarbeitung personenbezogener Daten (im Weiteren „Daten") durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung eines der folgenden Softwaremodule:

- Softwaremodule mit Rechnungs- und Buchhaltungsfunktionen gemäß der im Bestellprozess (Account-Registrierung) erworbenen lexoffice Versionen
- “Lohn & Gehalt”

Neben der Erhebung, Verarbeitung und Nutzung von Daten im Auftrag als Hauptzweck werden u.a. personenbezogene Daten im Rahmen der Kunden-, Lieferanten- und Personalverwaltung sowie für sonstige Zwecke (z.B. Geschäftspartner- und Interessentenbetreuung, Hilfe und Support, Analyse und Verbesserung des Dienstleistungsangebots von lexoffice, sowie nach vorheriger Einwilligung für Marketingmaßnahmen) erhoben, verarbeitet oder genutzt.

1.2 Dauer der Vereinbarung

Die Laufzeit dieses Vertrages entspricht der Laufzeit der Lizenzvereinbarung.

2. Konkretisierung des Auftragsverhältnisses

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Zweck der lexoffice Softwaremodule ist es, Klein- und Kleinstunternehmen bei der Durchführung ihrer Geschäftstätigkeit optimal zu unterstützen und zu entlasten. Hierbei erbringt lexoffice insbesondere Leistungen der Datenverarbeitung und der Telekommunikation sowie andere Dienstleistungen und Nebenleistungen. Der Auftragsverarbeiter erhält dabei Zugriff auf die bei der Benutzung der in den vertragsgegenständlichen Softwaremodulen gespeicherten personenbezogenen Daten und nutzt diese zum Zweck der Leistungserbringung und zu damit kompatiblen Zwecken unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO im Auftrag des Auftraggebers. Der Umfang der vorgenommenen Erhebung, Verarbeitung und Nutzung dieser Daten richtet sich dabei nach den Leistungen und dem Funktionsumfang des Produktes. Hierzu zählen auch die Verwendung und pseudonymisierte Auswertung von Daten zur Bereitstellung, Weiterentwicklung und Optimierung von Funktionalitäten des Produktes im Auftrag des Auftraggebers.

Folgende Datenkategorien können vom Verantwortlichen durch direkte Eingabe oder durch Hochladen in allen lexoffice Versionen verarbeitet werden:

Angaben zu Kunden und Lieferanten: Stammdaten wie Name und Anschrift, E-Mail-Adresse, Telefonnummer, Mobilfunknummer, Bankverbindung, Bestelldaten, Beleg-/ Rechnungsdaten (z.B. Belegdatum, Belegnummer, Betrag, Posten (inkl. Steuersätze), IBAN/BIC, Fälligkeitsdatum), Daten zum Zahlungsverhalten, Steuernummer / UST-ID Nr., Daten zum Zahlungsverhalten, Ansprechpartner

Angabe zu Mitbenutzern (User) in lexoffice: Anrede, Name, Vorname, E-Mail-Adresse, Zeitstempel und IP-Adresse des letzten Logins, durchgeführte Aktionen innerhalb von lexoffice (Audit Log)

Angaben zur Firma: u.a. Firmenname, Adresse, Name, Vorname, Telefonnummer, E-Mail-Adresse, Banktransaktionsdaten (z.B. IBAN/BIC, Betrag, Buchungstext, Verwendungszweck, Transaktionsdatum, Kontentyp), Sicherheitsfrage für Passwortverlust, Angaben zum Finanzamt, der Kirchensteuer, der Sozialversicherung, verschiedene Abrechnungsangaben

Im Modul “Kundenmanager” können Dateien mit kundenrelevanten Informationen hochgeladen werden. Die Verantwortung für diese Inhalte trägt allein der Verantwortliche. Insbesondere sind dort keine Dateien hochzuladen, die gegen die Lizenzvereinbarungen oder geltendes Recht verstoßen.

In der Version “Lohn & Gehalt” werden zusätzlich folgende Datenarten / -kategorien verarbeitet:

Mitarbeiterdaten: Adresse, Name, Vorname, Telefonnummer, E-Mailadresse, Firmenangaben, Tätigkeitsangaben, Meldeangaben, Sozialversicherungsangaben, Besteuerungsangaben (u.a. Familienstand, Anzahl Kinder), Angaben zur Vorbeschäftigung, zu Vorjahren, zu Vorträgen, IBAN/BIC, Angaben zur Krankenversicherung (u.a. Stammdaten der Krankenkasse und Beitragssätze, sämtliche Datenfelder / der Sozialversicherung / Lohnsteuerkarte (u.a. Merkmale der Religion zur Berechnung der Kirchensteuer)

Alle Kernfunktionen von lexoffice werden ausschließlich in Deutschland entwickelt und gehostet (Rechnungserstellung, Belegerfassung- und Verarbeitung, Lohnabrechnungen, Kassenfunktionen). Darüber hinaus gibt es ergänzende Zusatzfunktionen (z.B. E-Mail Versand, Supportplattform, Analytics), bei der auf durch den Verantwortlichen genehmigte Subunternehmen (siehe **Anlage 1**) zurückgegriffen wird, die teilweise ihren Sitz außerhalb der EU/EWR haben.

Jede weitere Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO).

2.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden und Lieferanten des Verantwortlichen
- Ansprechpartner bei Kunden und Lieferanten des Verantwortlichen
- Mitbenutzer (User), die durch den Verantwortlichen zur Mitarbeit in lexoffice freigeschaltet werden, z.B. der Steuerberater des Verantwortlichen oder eine Buchhaltungsfachkraft im Unternehmen des Verantwortlichen

In der Version “Lohn & Gehalt” zusätzlich:

- Beschäftigte des Verantwortlichen gem. § 26 Abs. 8 BDSG.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter verpflichtet externe Rechenzentren sowie sonstige Unterauftragsverarbeiter, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiter alle technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

3.2 Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen (Einzelheiten in **Anlage 2**).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter 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

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

4.2 Der Auftragsverarbeiter wird die Daten des Verantwortlichen nach dem Ende der Lizenzvereinbarung wie folgt behandeln:

1. Der Account bleibt in kostenlosem Read-Only Modus. Hilfeartikel: **„Sind meine Daten auch nach der Kündigung noch verfügbar?“**
2. Der Verantwortliche kann jederzeit vollständige Löschung verlangen (Self-Service). Hilfeartikel: **„Wie lösche ich meinen Account?“**
3. Der Verantwortliche kann jederzeit alle Daten in gängigen Datenaustauschformaten exportieren. Hilfeartikel: **Import / Export in lexoffice**
4. Entschließt sich ein Verantwortlicher nach der kostenlosen Testphase nicht zum Kauf eines lexoffice Abonnements, so wird der Testaccount nach einem

letztmaligen Hinweis per E-Mail automatisch spätestens 13 Monate nach Beendigung der Testregistrierung gelöscht.

Darüber hinaus sind zusätzliche Löschkonzepte, das Recht auf Vergessenwerden, die Berichtigung und Auskunft vom Verantwortlichen sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

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

1. Der Auftragsverarbeiter sichert zu, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt zu haben, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird.
2. Datenschutzbeauftragter des Auftragsverarbeiters ist: Raik Mickler, Telefon: 0761/898-0, E-Mail: **dsb@haufe-lexware.com**
3. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit (inklusive § 203 StGB) verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
4. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in **Anlage 2**).
5. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
6. Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.
7. Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
8. Der Auftragsverarbeiter 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.

9. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

10. Falls der Verantwortliche eine kirchliche Stelle ist, wird der Auftragsverarbeiter auch die für den Verantwortlichen geltenden speziellen Datenschutzvorschriften beachten und einhalten. Soweit in der jeweiligen Datenschutzvorschrift vorgesehen, unterwirft sich der Auftragsverarbeiter der für den Verantwortlichen zuständigen kirchlichen Datenschutzaufsicht.

6. Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice erbringt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter eine solchen Einschaltung von Unterauftragsverarbeitern dem Verantwortliche eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.

3. Der Verantwortliche stimmt der Beauftragung der in der **Anlage 1** vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

5. Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Drittanbieter

Wir bieten Kooperationen mit externen Partnern an (Details siehe AGBs). Der Auftraggeber (lexoffice Kunde) schließt mit diesen Partnern direkt Lizenzverträge und Verträge zur Auftragsverarbeitung ab. Stimmt der Auftraggeber der Datenübertragung an diese Partner zu, werden die Daten vom Auftragnehmer übertragen.

8. Kontrollrechte des Verantwortlichen

1. Der Verantwortliche hat nach Vorankündigung das Recht, die Einhaltung der über die datenschutzrechtlichen Prozesse und der vertraglichen Vereinbarung durch den Auftragsverarbeiter oder das externe Rechenzentrum/den Unterauftragsverarbeiter zu kontrollieren. Dies kann entweder durch die Einholung von Auskünften oder die Vorlage von aktuellen Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter) oder durch eine geeignete Zertifizierung mittels IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.
2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

9. Mitteilung bei Verstößen des Auftragsverarbeiters

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
   - die Verpflichtung, den Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   - die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung

- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

10.Weisungsbefugnis des Verantwortlichen

1. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

2. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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 Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Für die Löschung der Daten in der Applikation gilt Nr. 4.

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

12. Schlussbestimmungen

Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Unterzeichnung in Kraft und ersetzt alle zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung.

Anlage 1: Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Nr.	Firma	Anschrift	Leistung
1	Haufe-Lexware GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg	Entwicklung & Support
2	Haufe Lexware Services GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg	Technischer Anwendersupport & Auskunft
3	Amazon Web Services EMEA Sarl (“AWS Frankfurt”)	38 Avenue John F. Kennedy, L-1855 Luxembourg	Hosting und Betriebsaufgaben für alle Rechnungs- und Buchhaltungsfunktionen der im Bestellprozess (Account-Registrierung) erworbenen lexoffice Versionen
3a	Amazon Web Services Inc.	410 Terry Avenue North, Seattle WA 98109, United States	Nur mit vorheriger Genehmigung für interne Support-Leistungen von AWS ggü. lexoffice
4	UserVoice Inc.	121 2nd St, Floor 4, San Francisco, CA 94105, USA	Hosting und Betrieb eines von der Applikation unabhängigen Feedbacktools für alle lexoffice Versionen

Nr.	Firma	Anschrift	Leistung
5	The Rocket Science Group LLC	675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308 USA	Versand aller Arten von E-Mails mit der Applikation “Mandrill“ für alle lexoffice Versionen
6	Intercom Inc.	55 2nd Street, 4th Floor, San Francisco, California, 94105, USA	Hosting und Betrieb eines Webanalyse- und Kommunikationsdienstes für alle lexoffice Versionen
7	Insiders Technologies GmbH	Brüsseler Str. 1, 67657 Kaiserslautern	Datenextraktion aus Buchungsbelegen für alle lexoffice Versionen
8	B+S Banksysteme AG	Elsenheimerstraß e 45, 80687 München	Einheitliche Schnittstelle zum Abruf von Online-Banking Informationen für alle lexoffice Versionen
9	SorryApp Ltd.	Mclarens, Penhurst House, 352-6 Battersea Park Road, London, England, SW11 3BY	Statusmeldungen zu einzelnen lexoffice Funktionen (bspw. Verfügbarkeit technischer Services)
10	BANKSapi Technology GmbH	Lyonel-Feininger-Str. 28, 80807 München	Einheitliche Schnittstelle zum Abruf von Online-Banking Informationen für alle lexoffice Versionen
11	Klippa App B.V.	Laan Corpus den Hoorn 1, 9728 JM Groningen, Netherlands	Datenextraktion aus Buchungsbelegen für alle lexoffice Versionen

Anlage 2: Technische und organisatorische Maßnahmen

der Haufe Service Center GmbH, Haufe-Lexware GmbH & Co. KG und Haufe Lexware Services GmbH & Co. KG

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle:

- Gebäude allgemein:
  – Alle Mitarbeiter:innen und jeder Besucher trägt sichtbar einen Firmen/Besucherausweis, der zudem eine Schlüsselfunktion (Chipkarte) enthält, über den der Zugang zu Gebäuden beschränkt wird
  – Besucher müssen sich bei ihrer Ankunft an- und bei ihrer Abreise abmelden. Während ihres Aufenthalts werden sie von Mitarbeiter: innen begleitet.
  – Die Gebäude werden videoüberwacht.
  – Ein Sicherheitsdienst überwacht die Gebäude und das Gelände außerhalb der Bürozeiten
- Rechenzentrumsräume:
  – lexoffice Kundendaten werden in Rechenzentren von AWS Frankfurt verarbeitet und gespeichert

1.2 Zugangskontrolle:

- Der Benutzer- und Administratorzugriff auf das lexoffice System beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Es existieren technische Policies zur Passwortkomplexität.
- Bei lexoffice gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Einsatz von Firewallsystemen, Virenscanner und Intrusion Detection Systemen auf lexoffice Serversystemen
- Der Zugriff auf lexoffice Serversysteme erfolgt SSH-verschlüsselt („Public key“) durch einen Bastion-Host, was den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt.
- Alle lexoffice Serversysteme speichern Daten ausschließlich auf verschlüsselten Datenträgern ab.

1.3 Zugriffskontrolle:

- Zugriffsberechtigung auf lexoffice Produktivsysteme ist auf einen kleinen Kreis von Mitarbeiter:innen (“lexoffice Systemadministrator:innen”) beschränkt
- Alle Zugriffe auf lexoffice Produktivsysteme durch lexoffice Systemadministratoren werden mit User-ID, Zeitstempel und Anlass protokolliert und GoBD-konform für 10 Jahre aufbewahrt
- lexoffice Systemadministratoren haben ausschließlich lesenden Zugriff auf die Zugriffsprotokolle
- Es existiert ein internes Kontrollsystem, das sicherstellt, dass die Rechtmäßigkeit für Zugriffe auf lexoffice Produktivsysteme regelmäßig stichprobenartig überprüft und diese Stichprobenkontrollen ebenfalls protokolliert werden

1.4 Trennungskontrolle:

- Datensätze unterschiedlicher lexoffice Kunden werden in einer einheitlichen Datenbank speziell markiert (Tenant-ID, softwareseitige Mandantenfähigkeit). Vgl. dazu auch jeweils aktuelles GoBD-Testat.
- Test- und Produktivdaten sind strikt getrennt in unabhängigen Systemen, Entwicklungssysteme sind ebenfalls unabhängig von Test- und Produktivsystemen
- Unterschiedliche Domains und SSL-Zertifikate für Test- und Produktivsysteme

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

2.1 Weitergabekontrolle:

- Datenübertragung zwischen lexoffice Serversystemen erfolgt ausschließlich innerhalb abgegrenzter und durch Bastion-Hosts abgeschirmter Subsysteme
- Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer TLS verschlüsselt
- Wo dies technisch möglich ist, kommen VPN-Verbindungen zum Einsatz
- Datenabrufe und Übermittlungsaktivitäten werden protokolliert

2.2 Eingabekontrolle:

- GoBD-konformes Audit-Log als Feature in lexoffice, in dem Eingaben durch Kunden protokolliert und 10 Jahre GoBD-konform aufbewahrt werden.

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

3.1 Verfügbarkeitskontrolle:

- Es werden regelmäßig automatische Sicherungskopien und Backups aller lexoffice Kundendaten erstellt
- Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Es existiert ein Notfallkonzept für lexoffice mit namentlich benannten Verantwortlichen und einer expliziten Vertreterregelung.
- Das Notfallkonzept wird regelmäßig überprüft und aktualisiert
- Mitarbeiter:innenwerden in regelmäßigen Abständen auf dieses Notfallkonzept geschult.
- Backups und Sicherungskopien sind über mehrere redundante Serversysteme und Rechenzentrumsstandorte verteilt
- lexoffice Produktivsysteme sind mehrfach redundant ausgelegt

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):

- Mehrfach-redundante Auslegung von Serversystemen und Datenbanken
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft
- Es gibt regelmäßige Notfallübungen, in denen Teams u.a. Wiederherstellungsszenarien üben

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

4.1 Für sämtliche Unternehmen in der Haufe Group in denen personenbezogenen Daten verarbeitet werden, wurde ein Datenschutzbeauftragter bestellt. Die Haufe Group hat die Grundsätze des Datenschutzes in einer Datenschutzrichtlinie festgelegt.

4.2 Die Haufe Group verfügt über ein Datenschutzmanagementsystem. Mit entsprechender Planung zu Maßnahmen zum Umgang mit Chancen/Risiken und die Ausstattung mit angemessenen Ressourcen, Kompetenzen, Awareness und Kommunikation. Die Überwachung, Messung, Analyse und Bewertung, zusammen mit internen Audits und Managementbewertungen finden zur fortlaufenden Verbesserung des Managementsystems kontinuierlich statt. Das Managementsystem des Auftragsverarbeiter ist bei den Hostern integriert.

4.3 Dediziertes Incident-Response-Management für lexoffice (Vgl. §3)

4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

4.5 Auftragskontrolle:

- Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen
- Klare, eindeutige Weisungen
- Verhinderung von Zugriffen unbefugter Dritter auf die Daten
- Verbot, Daten in unzulässiger Weise zu kopieren
- Vereinbarungen über Art des Datentransfers und deren Dokumentation
- Kontrollrechte durch den Auftraggeber
- Vereinbarung von Vertragsstrafen
- strenge Auswahl der Dienstleister
- Nachkontrollen

Stand: 26.03.2024