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

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.

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, Marktanalysen und Marketingmaßnahmen) erhoben, verarbeitet oder genutzt.

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"

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 in Ausnahmefällen außerhalb der EU/EWR ihren Sitz haben sind. 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 BDSG (neu).

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.

Die technischen und organisatorischen Maßnahmen in **Anlage 2** machen aufgrund der Schnelllebigkeit der Technik kontinuierliche Verbesserungen und diesbezügliche Anpassungen (Änderungen und Aktualisierungen) erforderlich, über die wir entsprechend informieren.

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:

a. Der Account bleibt in kostenlosem Read-Only Modus. Hilfeartikel: **„Sind meine Daten auch nach der Kündigung noch verfügbar?“**
b. Der Verantwortliche kann jederzeit vollständige Löschung verlangen (Self-Service). Hilfeartikel: **„Wie lösche ich meinen Account?“**
c. Der Verantwortliche kann jederzeit alle Daten in gängigen Datenaustauschformaten exportieren. Hilfeartikel: **Import / Export in lexoffice**
d. 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 60 Tage nach Beendigung der kostenlosen Testphase 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:

a. Der Auftragsverarbeiter sichert zu, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt zu haben, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird.

b. Datenschutzbeauftragter des Auftragsverarbeiters ist: Raik Mickler, Telefon: 0761/898-0, E-Mail: **dsb@haufe-lexware.com**

c. 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.

d. 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**).

e. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f. 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.

g. 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.

h. 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.

i. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

a. 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 sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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.

b. 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.

c. 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.

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

e. 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

a. 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 Verantwortliche auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

b. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortlicher von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlicher auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

9. Mitteilung bei Verstößen des Auftragsverarbeiters

a. 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

b. 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

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

b. 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

a. 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.

b. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlicher – 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.

c. 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

a. Änderungen und Ergänzungen dieser Vertragsregelung und all ihrer Bestandteile, einschließlich etwaiger Zusicherungen des Auftragsverarbeiters, bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vertragsregelung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

b. Sollten einzelne Teile dieser Vertragsregelung unwirksam sein, so berührt dies die Wirksamkeit der Vertragsregelung im Übrigen nicht. An Stelle der unwirksamen Bestimmung soll eine Bestimmung vereinbart werden, die dem von den Partnern hiermit verfolgten wirtschaftlichen Zweck möglichst nahekommt. Entsprechendes gilt im Falle einer Regelungslücke.

c. Diese Vertragsregelung unterliegt ausschließlich dem formellen und materiellen Recht der Bundesrepublik Deutschland. Die Anwendung des internationalen Privatrechts sowie des einheitlichen UN-Kaufrechts (CISG) wird ausdrücklich ausgeschlossen.

d. Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Unterzeichnung in Kraft.

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 & Marketing
2	Haufe Lexware Services GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg	Technischer Anwendersupport & Auskunft
3	Amazon Web Services Inc. (“AWS Frankfurt”)	410 Terry Avenue North, Seattle WA 98109, United States	Hosting und Betriebsaufgaben für alle Rechnungs- und Buchhaltungsfunktionen der im Bestellprozess (Account-Registrierung) erworbenen lexoffice Versionen
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
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	Elsenheimerstraße 45, 80687 München	Einheitliche Schnittstelle zum Abruf von Online-Banking Informationen für alle lexoffice Versionen
9	Google Inc.	Amphitheatre Parkway, Mountain View, CA 94043, USA	Interne und externe Kommunikation über E-Mail und G-Suite Office
10	SorryApp Ltd.	Mclarens, Penhurst House, 352-6 Battersea Park Road, London, England, SW11 3BY	Statusmeldungen zu einzelnen lexoffice Funktionen (bspw. Verfügbarkeit technischer Services)

Anlage 2: Technische und organisatorische Maßnahmen

1. Technische und organisatorische Maßnahmen der Haufe Group SE Unternehmen: 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
    - Technische und organisatorische Maßnahmen bei AWS Frankfurt sind in **Anlage 2** zu diesem Vertrag aufgeführt
    -

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
- Für Admin-Zugriffe durch Dienstleister (AWS Frankfurt): Siehe Technische und organisatorische Maßnahmen bei AWS Frankfurt in **Anlage 2** zu diesem Vertrag.

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
- Zur Ausstattung der Rechenzentren von AWS Frankfurt, vgl. Technische und organisatorische Maßnahmen bei AWS Frankfurt in **Anlage 2** zu diesem Vertrag

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

2. Technische und organisatorische Maßnahmen: Amazon Web Services Inc.

Es wurden alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO ergriffen.

3. Technische und organisatorische Maßnahmen: UserVoice

Aufgrund der Schnelllebigkeit der Technik verweisen wir aus Gründen der Praktikabilität und Aktualität sowie zum Zweck der Wahrung der Unverfälschtheit der Informationen auf die Originalsprache (Englisch) der offiziellen Quelle dieses Unterauftragsverarbeiters:

https://uservoice.com/security-compliance

4. Technische und organisatorische Maßnahmen: The Rocket Science Group

Aufgrund der Schnelllebigkeit der Technik verweisen wir aus Gründen der Praktikabilität und Aktualität sowie zum Zweck der Wahrung der Unverfälschtheit der Informationen auf die Originalsprache (Englisch) der offiziellen Quelle dieses Unterauftragsverarbeiters:

https://mailchimp.com/about/security

5. Technische und organisatorische Maßnahmen: Intercom Inc.

Aufgrund der Schnelllebigkeit der Technik verweisen wir aus Gründen der Praktikabilität und Aktualität sowie zum Zweck der Wahrung der Unverfälschtheit der Informationen auf die Originalsprache (Englisch) der offiziellen Quelle dieses Unterauftragsverarbeiters:

https://www.intercom.com/de/legal/data-processing-agreement

6. Technische und organisatorische Maßnahmen: Insiders Technologies

1 Vorbemerkung

Insiders setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den getroffenen Vereinbarungen erfolgt.

2 Spezielle Maßnahmen für Rechenzentrumsbetrieb der Cloud-Lösungen

2.1 Insiders nutzt für den Betrieb der Cloud-Lösungen und die Erbringung der damit verbundenen Services die Leistungen eines oder mehrere externe Rechenzentren. Für jedes solches Rechenzentrum hat Insiders mit dem jeweiligen Rechenzentrumsbetreiber eine Vereinbarung über Auftragsverarbeitung abgeschlossen, in der eigene, speziell auf den Rechenzentrumsbetrieb ausgerichtete technische und organisatorische Maßnahmen festgelegt sind.

2.2 Die für den Rechenzentrumsbetrieb der Cloud-Lösungen geltenden technischen und organisatorischen Maßnahmen sind in Anlage 1a beschrieben. Auf die übrige Verarbeitung personenbezogener Daten durch Insiders finden die in den folgenden Ziffern 3 bis 7 beschriebenen technischen und organisatorischen Maßnahmen Anwendung.

Die technischen und organisatorischen Maßnahmen beziehen sich auf die Maßnahmen bei Insiders, jeweils erforderlichenfalls ergänzt um zusätzlich umgesetzte Maß nahmen im externen Rechenzentrum für Colocation/Housing und/oder um zusätzlich umgesetzte Maßnahmen in der Cloud-Umgebung bei Insiders.

3 Kundendaten

3.1 Für den Support der Cloud-Lösung kann es erforderlich sein, dass Kunden Insiders Beispieldokumente (Rechnungen, Lieferscheine, Formulare etc.) und Stammdaten zur Verfügung stellen.

3.2 Alle Insiders von Kunden im Sinne von Ziffer 3.1 überlassenen Daten werden zentral im Support verwaltet. Datenträger und Dokumente in Papierform werden zugriffssicher verschlossen gelagert. Elektronische Dokumente werden zentral

und logisch getrennt abgelegt. Für die Ablage von Kundendaten stehen dedizierte Fileserver und Datenbankserver in einem externen Rechenzentrum zur Verfügung.

3.3 Die Ablage dieser Daten erfolgt zu Sicherheitszwecken in pseudonymisierter Form. Die Zuordnung von Daten zu Kunden erfolgt hierbei über Supportmitarbeiter. Als weitere Sicherheitsmaßnahme werden die Kundendaten Fileserver-basiert auf einem hardwareverschlüsselten Plattensystem abgelegt.

3.4 Zugriff auf die Kundendaten erhalten nur autorisierte Mitarbeiter und auch diese ausschließlich für die jeweils benötigten Kundendaten. Hierzu werden für elektronische Dokumente auf Dateiebene Rechte für die entsprechenden Benutzer festgelegt. Papierdokumente werden nur gegen Unterschrift herausgegeben. Für Mitarbeiter, die Zugriff auf Kundendaten benötigen, existiert ein dezidiertes Berechtigungskonzept, das im Falle sich ändernder Anforderungen angepasst wird.

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

4.1 Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:
- Alarmanlage
- Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher / Tragen von Besucherausweisen
- Begleitung von Besuchern
- Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Zutrittsbeschränkung zu Sicherheitszonen

Zusätzlich zu den vorstehenden Maßnahmen im externen Rechenzentrum für Colocation/Housing umgesetzte Maßnahmen:
- Mehrstufiges Zugangskontrollsystem
- Zugang über Pförtnerdienst

- Videoüberwachung im Eingangsbereich zum und im Rechenzentrum
- Einbruchmeldeanlage und Einsatz eines Sicherheitsdienstes

4.2 Zugangskontrolle:

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Es existieren folgende Maßnahmen zur Zugangskontrolle:
- Zuordnung von Benutzerrechten
- Verwendung von Benutzerrollen
- Passwortvergabe
- Automatische Sperrung von Accounts nach mehrfacher Fehleingabe
- Automatische Bildschirmsperre
- Verwendung von Passwort-Richtlinien
- Authentifikation mit Benutzername/Passwort
- Einsatz von Intrusion-Prevention-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie mit mehrstufiger Authentifizierung
- Einsatz von Software-Firewalls
- Protokollierung von Benutzeranmeldungen
- Verwendung von Netzwerksicherheitszonen

Zusätzlich zu den vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:
- Verschlüsselung von Daten im Filesystem
- Verschlüsselung von Datenbankinhalten
- Verwendung von IP-Filtern

4.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

- Protokollierung von An-/Abmeldungen am Active Directory
- Einsatz eines Intrusion-Prevention-System (IPS)
- Hardwareverschlüsselte Platten bei allen PCs und Laptops
- physische Löschung von Datenträgern vor Wiederverwendung
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399, Schutzklasse 2, Sicherheitsstufe H4)
- Ordnungsgemäße Vernichtung von Papierunterlagen (DIN 66399, Schutzklasse 3, Sicherheitsstufe P4)
- Protokollierung der Vernichtung

Zusätzlich zu den vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:

- Abgestufte Administrationsberechtigungen
- Einsatz eines IP-Filter für den Zugriff auf Cloud Anwendungen
- Applikationsseitige Verschlüsselung von datenschutzrelevanten Daten
- Administrative Zugriffe nur über SSL-VPN Verbindungen mit mehrstufiger Authentifizierung
- Protokollierung von An-/Abmeldungen
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Regelmäßige Penetrationstests aller Cloud Anwendungen

4.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Verwendung dedizierter File- und Datenbankserver
- Ablage bereitgestellter Supportdaten in pseudonymisierter Form
- Logische Mandantentrennung (softwareseitig)

Zusätzlich zu den vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:

- Verwendung von Row-Level-Security auf Datenbankebene
- Trennung von Entwicklungs-/Test- und Produktivsystemen
- Kundenspezifische Verschlüsselung von Anwendungsdaten
- Kundenspezifische Matching-Datenbanken

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

5.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Es existieren folgende Maßnahmen zur Weitergabekontrolle:
- E-Mail-Verschlüsselung (TLS-Verschlüsselung)
- Absicherung der Online-Datentransfers durch geschützte Übertragungswege (HTTPS, VPN)
- Regelungen (u.a. arbeitsrechtliche) für den Umgang mit Daten und IT Strukturen
- Weitergabe von Kundendaten ausschließlich auf Weisung des Kunden

Zusätzlich zu den vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:
- Beschränkung des Hochladens von Dokumenten und Abholens von Ergebnissen auf registrierte Kundensysteme
- Einrichtungen von Standleitungen bzw. VPN-Tunneln

5.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.
Es existieren folgende Maßnahmen zur Eingabekontrolle:
- Für Support- und Entwicklungszwecke für Kunden werden nur Test- und Entwicklungssysteme eingesetzt. Zusätzlich zu den vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:
- Betrieb von Produktiv-, Entwicklungs- und Testsystemen für Kunden
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung alle API-Aufrufe der smart Cloud

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

6.1 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. c) DSGVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-

Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Verwendung von Hardwareredundanzen
- Verwendung von Clustern (VMWare, Datenbanken etc.)
- Verwendung von Virenscannern
- Verwendung von Firewalls
- Asynchron gespiegelte Storage-Systeme
- Rauchmelder

Zusätzlich zu den vorstehenden Maßnahmen im externen Rechenzentrum für Colocation/Housing umgesetzte Maßnahmen:
- Unterbrechungsfreie Stromversorgung (USV)
- Notstromversorgung über Dieselgenerator
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Redundante Kälte- und Klimaversorgung
- Brandmeldesysteme mit Früherkennung
- Gaslöschanlage
- Schutzsteckdosenleisten in Serverräumen
- Anbindung über redundante, dedizierte Glasfaserstrecken

Zusätzlich zu allen vorstehenden Maßnahmen in Cloud-Umgebung bei Insiders umgesetzte Maßnahmen:
- Redundante Produktivumgebung
- Synchron gespiegelte Storage Systeme

6.2 Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) GDPR)

Es existieren folgende Maßnahmen zur raschen Wiederherstellung:
- Tägliche automatische Snapshoterstellung
- Bei Changes: gesonderte, manuelle Snapshoterstellung
- Automatische Erstellung von Datenbankdumps

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

Es existieren folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- Datenschutz-Management
- Prüfung der vertraglichen Regelungen mit Mitarbeitern und ggf. Mitarbeitern externer Dienstleister
- Vertraulichkeitsvereinbarung;
- Belehrung und Verpflichtung auf das Datengeheimnis sowie das Sozialgeheimnis gemäß Sozialgesetzbuch (§ 35 SGB I und § 80 SGB X);
- Vereinbarung über die Nutzung der IT- und TK-Infrastruktur;
- Sicherung der Urheberrechte bei Insiders bzw. beim Kunden, sofern dies vereinbart ist;
- Belehrung und Verpflichtung auf weitere datenschutzrelevante Vorschriften und Gesetze, insbesondere das Postgeheimnis gemäß Postgesetz (§§ 39, 41 PostG), das Fernmeldegeheimnis gemäß Telekommunikationsgesetz (§ 88 TKG) sowie § 203 StGB.
- Regelmäßige Datenschutzschulungen
- Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der getroffenen Maßnahmen
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Überprüfung des Auftragnehmers und seiner Tätigkeiten

Zum Zeitpunkt der Erstellung dieses Dokumentes können die folgenden Zertifizierungen nachgewiesen werden:

- ISO/IEC 27001:20l3, Zertifikat-Registrier-Nr. 73 121 6688

- ISO/IEC 27001:20l3, Zertifikat-Registrier-Nr. 16-I-0000007-TIC (Externes Rechenzentrum für Colocation/Housing)

Anlage 1a: Technische und organisatorische Maßnahmen – Rechenzentrum Cloud-Betrieb

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:
- Alarmanlage
- Automatisches Zugangskontrollsystem
- Schließsystem mit Codesperre
- Lichtschranken/Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner/Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen

1.2 Zugangskontrolle:

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Es existieren folgende Maßnahmen zur Zugangskontrolle:
- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Sperren von externen Schnittstellen (USB etc.)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal

- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Software-Firewall

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:
- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399, Schutzklasse 3)
- Protokollierung der Vernichtung

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Es existieren folgende Maßnahmen zur Trennungskontrolle:
- Erstellung eines Berechtigungskonzepts

- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Trennung von Entwicklungs-/Test- und Produktivsystemen

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a) DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher
Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese
zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und
organisatorischen Maßnahmen unterliegen

Es existieren folgende Maßnahmen zur Pseudonymisierung:
- Im Rahmen eines Angebotes wird im ausgewiesenen CRM System eine eindeutige ID erzeugt. Diese ID wird von den mit den folgenden Verarbeitungsschritten betrauten Rollen als eindeutige Identifikation verwendet. Aus einer oder mehreren ID’s lassen sich keine Rückschlüsse auf Betroffene ziehen.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Es existieren folgende Maßnahmen zur Weitergabekontrolle:
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung (TLS-Verschlüsselung)
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Es existieren folgende Maßnahmen zur Eingabekontrolle:
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. c) DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:
- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen

3.2 Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) GDPR)

Es existieren folgende Maßnahmen zur raschen Wiederherstellung:
- Tägliche automatische Snapshoterstellung
- Auf Dateiebene: Sicherungskonzepte für Wiederherstellung einzelner Dateien auf Generationenprinzipbasis
- Bei Changes: gesonderte, manuelle Snapshoterstellung

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

Es existieren folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung:
- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafen bei Verstößen
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Technische und organisatorische Maßnahmen: B+S AG

Zutrittskontrolle
- Tür „offen“-Alarm: Automatische Überwachung der Türöffnungszeiten.
- Begehung der Serverräume: Monatliche Kontrolle der Begehungsprotokolle.
- Zentrales Zugangssystem: Zentrales Zugangssystem mit starker Drei-Phasen Authentifizierung – ID Card, biometrischer Abfrage und Code im Hochsicherheitsbereich und starker Zwei-Phasen Authentifizierung – ID Card und Code – in den Büroräumlichkeiten.
- Alarmanlagen und Bewegungsmelder: Absicherung des Rechenzentrums mittels Alarmanlagen und Bewegungsmeldern.
- Videoüberwachung des Zutrittsbereichs: Laufende Videoüberwachung im Rechenzentrum und im Zutrittsbereich.
- Besucherbuchkontrolle: Regelmäßige Kontrolle des Besucherbuches.

Zugangskontrolle

- IT-Security Awareness Schulungen: IT-Security Awareness Schulungen aller Mitarbeiter.
- Automatische Überwachung der Anmeldungen: Automatische Überwachung des Anmeldeverfahrens und Alarmierung bei unerlaubten Zugriffen.
- Freigabe der Userberechtigungen: Nur ein eingeschränkter Userkreis hat die Möglichkeit, sich auf den Systemen anzumelden. Diese Userrechte werden regelmäßig geprüft.
- Fernwartung Überprüfung der Fernwartungsprotokolle.
- Automatische Sperrung der Workstations: Alle Workstations werden nach 10 Minuten der Inaktivität automatisch gesperrt.
- Clean Desk Prüfung: Stichprobenartige Überprüfung der Clean Desk Policy.
- Überprüfung der Passwortsecurity: Es wird geprüft, ob die betroffenen Windows Systeme am zentralen AD angebunden sind und hierbei die Passwortkompolexitätspolicy eingehalten wird. Bei den betroffenen Linux und UNIX Systemen wird die Mindestpasswortkomplexität über die AD Authentifizierung sichergestellt.
- Überprüfung des Austrittsprozesses: Es wird sichergestellt, dass bei einem Austritt alle
Berechtigungen des jeweiligen Mitarbeiters zeitnah gesperrt und sämtliche Passwörter, von denen der jeweilige Mitarbeiter Kenntnis hatte, geändert werden.
- Überprüfung der Userberechtigungen: Nur ein eingeschränkter Userkreis hat die Möglichkeit, sich auf den Systemen anzumelden. Diese Userrechte werden regelmäßig geprüft.

Zugriffskontrolle

- Prüfung der Userberechtigungen im Ticketsystem: Wiederkehrende Überprüfung der Anmeldeberechtigungen und Rollenzuordnungen.
- Automatische Überwachung der Anmeldungen: Automatische Überwachung des Anmeldeverfahrens und Alarmierung bei unerlaubten Zugriffen.
- Automatische Viren Überwachung: Schutz der IT-Systeme durch Antivirensoftware;
automatisierte Überwachung in Bezug auf Wirksamkeit und Aktualität.
- Firewalländerungen im Augen-Prinzip: Jede Firewalländerung erfolgt im Augen-Prinzip.
- Freigabe der Userberechtigungen: Nur ein eingeschränkter Userkreis hat die Möglichkeit, sich auf den Systemen anzumelden; diese Userrechte werden regelmäßig geprüft.
- Kabelkontrolle: Überprüfung der Verkabelung.
- Fernwartung Überprüfung der Fernwartungsprotokolle.

- Automatische Sperrung der Workstations: Alle Workstations werden nach 10 Minuten der Inaktivität automatisch gesperrt.
- Clean Desk Prüfung: Stichprobenartige Überprüfung der Clean Desk Policy.
- Funktionsprüfung Helix (Protokollierung): Funktionsprüfung TestTrack (Protokollierung, Sperrung, Audittrail).
- Überprüfung der Passwortsecurity: Es wird geprüft, ob die betroffenen Windows Systeme am zentralen AD angebunden sind und hierbei die Passwortkomplexitätspolicy eingehalten wird. Bei den betroffenen Linux und UNIX Systemen wird die Mindestpasswortkomplexität über die AD Authentifizierung sichergestellt.
- Überprüfung des Austrittsprozesses: Es wird sichergestellt, dass bei einem Austritt alle Berechtigungen des jeweiligen Mitarbeiters zeitnah gesperrt und sämtliche Passwörter, von denen der jeweilige Mitarbeiter Kenntnis hatte geändert, werden.
- Überprüfung der Userberechtigungen: Nur ein eingeschränkter Userkreis hat die Möglichkeit, sich auf den Systemen anzumelden. Diese Userrechte werden regelmäßig geprüft.
- Überprüfung der VPN Zugänge: Es wird geprüft, ob die Nachvollziehbarkeit von VPN Client IP-Adressen bei Remote VPN Zugängen gegeben ist.
- Überprüfung der eingesetzten Software: Es wird überprüft, ob nur freigegebene Software auf Notebooks und Workstations eingesetzt wird.
- Überprüfung der Security Updates: Es wird geprüft, ob Security Updates regelmäßig eingespielt werden.
- Rezertifizierung der Virenüberwachung: Alle Festplatten von Datensicherungs- und Storagesystemen müssen verschlüsselt sein.

Verschlüsselung

- Prüfung der Festplattenverschlüsselung:Überprüfung der Festplattenverschlüsselung.
- Überprüfung der Emailverschlüsselung: Manuelle Überprüfung der Emailverschlüsselung.
- Überprüfung der Festplattenverschlüsselung von Datensicherungs- und Storagesystemen: Alle Festplatten von Datensicherungs- und Storagesystemen müssen verschlüsselt sein.

Trennungskontrolle

- Datenschutzschulung: Mitarbeiterschulung zu aktuellen Themen im Bereich Datenschutz.
- Weiterbildung der Datenschutzbeauftragten: Regelmäßige Weiterbildung der internen Datenschutzbeauftragten.

- Überprüfung der Ticketzuweisungen an die Kunden: Stichprobenartige Überprüfung der im TestTrack erfassten Kunden Issues.

Weitergabekontrolle

- Auslagerung der Sicherungsbänder: Die auf den TSM-Bändern gespeicherten Sicherungen werden zweimal pro Woche ausgelagert.
- Prüfung der Festplattenverschlüsselung: Überprüfung der Festplattenverschlüsselung.
- IT-Security Awareness: Schulungen

IT-Security Awareness: Schulungen aller Mitarbeiter.

- Automatische Viren Überwachung: Schutz der IT-Systeme durch Antivirensoftware; automatisierte Überwachung in Bezug auf Wirksamkeit und Aktualität.
- Firewalländerungen im Augen-Prinzip: Jede Firewalländerung erfolgt im Augen-Prinzip.
- Inventarprüfung der ausgelagerten Sicherungsbänder: Jährliche Bestandsprüfung der in der Bank hinterlegten Sicherungen.
- Datenträgerinventur: Die Datenträgerbestände werden durch Inventur überprüft.
- Datenträgervernichtung: Sicherstellung einer ordnungsgemäßen Datenträgervernichtung.
- Weiterbildung des Information Security Managers: Laufende Weiterbildungen des IT-Risk Managers durch den Berufsverband der internationalen IT-Auditoren der ISACA.
- Funktionsprüfung Helix (Protokollierung): Funktionsprüfung TestTrack (Protokollierung, Sperrung, Audittrail).
- Überprüfung der Email Postfächer: Stichprobenartige Überprüfung der Outlook Postfächer.
- Löschungsbestätigung: Prüfung der Löschbestätigung im TestTrack.
- Einspielkontrolle: Überprüfung ob personenbezogene Daten ausschließlich an definierten Orten aufbewahrt/eingespielt werden.
- Manuelle Löschprüfung (Datenschutzverzeichnis): Automatisches Löschen von kurzfristigen Datenschutzverzeichnissen.
- Überprüfung von Vereinbarungen: Es wird geprüft, ob alle Mitarbeiter eine Verschwiegenheitsvereinbar ung unterschrieben haben und ob all jene Mitarbeiter, die Zutritt zum Hochsicherheitsbereich erhalten haben, über die Videoaufzeichnung unterrichtet wurden.
- Überprüfung der Emailverschlüsselung: Manuelle Überprüfung der Emailverschlüsselung.
- Rezertifizierung der Virenüberwachung: Alle Festplatten von Datensicherungs- und Storagesystemen müssen verschlüsselt sein.

Eingabekontrolle

- Funktionsprüfung Helix (Protokollierung): Funktionsprüfung TestTrack (Protokollierung, Sperrung, Audittrail).
- Einspielkontrolle: Überprüfung ob personenbezogene Daten ausschließlich an definierten Orten aufbewahrt/eingespielt werden.
- Manuelle Löschprüfung (Datenschutzverzeichnis): Automatisches Löschen von kurzfristigen Datenschutzverzeichnissen.

Verfügbarkeitskontrolle

- Prüfung der Notfalldokumentation: Jährliche Kontrolle des IT Notfallkonzeptes, der Notfallleitlinie sowie der technischen DRP Dokumentation.
- Business Impact Analyse: Prüfung ob alle Technical Mapped Services des Service-Katalogs in der Business Impact Analyse vorhanden sind und seitens der Geschäftsführung bewertet wurden.
- Kontrolle und Funktionsprüfung des Krisenstabsraumes: Kontrolle und Funktionsprüfung der Ausrüstung des im Notfallkonzept angeführten Krisenstabsraumes.
- Disaster Recovery Tests Durchführung von IT Kontinuitätstests, inklusive Mitarbeiterbewertung, Review und Lessons Learned.
- Auslagerung der Sicherungsbänder: Die auf den TSM-Bändern gespeicherten Sicherungen werden zweimal pro Woche ausgelagert.
- Überprüfung der Datensicherungen: Monatlich werden die Tagesprotokolle stichprobenartig kontrolliert.
- Automatische Fehlererkennung des Kernsystems: Jährliche Überprüfung der Automatischen Fehlererkennung.
- Überwachung der synchronen Datenbankspiegelung: Automatische Überwachung der synchronen Datenbankspiegelung zwischen den Standorten.
- Kontrolle der TSM Sicherungseinstellungen: Prüfung des Sicherungsbedarfs von vorhandenen Filesystemen.
- Kompatibilitätstest der LTO-Sicherungsbänder: Jährlicher Kompatibilitätstest mit den unterschiedlichen Typen von LTO Sicherungsbändern.
- Inventarprüfung der ausgelagerten Sicherungsbänder: Jährliche Bestandsprüfung der in der Bank hinterlegten Sicherungen.
- Wiederherstellung von Rücksicherungen: Regelmäßige Rücksicherungstests.
- Begehung der Serverräume: Monatliche Kontrolle der Begehungsprotokolle.
- Überwachung der Temperatur an den RZ Standorten: Überprüfung der Automatischen Feuer- und Wassermelder.
- Überwachung der Verbindung zwischen den Rechenzentren: Redundante Netzwerkverbindung zwischen den getrennten RZ-Standorten.
- Schulung der operativen Abläufe: Regelmäßige Schulungen der im Betriebshandbuch definierten Abläufe.

- Automatisches Monitoring: Nagios-Überwachung mit Automatischer Email Benachrichtigung.
- Kontrolle der Wartungsverträge: Monatliche Kontrolle aller Wartungsverträge, die für die produktive Umgebung essentiell sind.

Auftragskontrolle

- Risk Assessment: Regelmäßiger Risk Assessment mit detaillierter Risikobeschreibung.
- Funktionsprüfung Helix (Protokollierung): Funktionsprüfung TestTrack (Protokollierung, Sperrung, Audittrail).
- Prüfung der Vereinbarungen mit Kunden: Kontrolle, ob die ADVs mit Auftraggebern eingehalten werden.
- Prüfung der Vereinbarungen mit Dienstleistern: Kontrolle, ob die ADVs mit den Dienstleistern aktuell und ausreichend sind.
- Überprüfung von Dienstleistern: Überprüfung der technischen und organisatorischen
Maßnahmen von Dienstleistern.
- Konzerninterne Prüfung der ADV auf Aktualität: Kontrolle, ob die konzerninternen ADVs aktuell und ausreichend sind.

Allgemeine Verfahren/Data Breach

- Security Incident Behandlung: Qualifizierte und professionelle Security Incident Behandlung gemäß CSIR-Plan.
- IT-Security Compliance Audit: Kontrolle, ob alle Security und Compliance Vorgaben eingehalten werden.
- Datenschutzschulung: Mitarbeiterschulung zu aktuellen Themen im Bereich Datenschutz.
- Weiterbildung der Datenschutzbeauftragten: Regelmäßige Weiterbildung der internen Datenschutz beauftragten.
- Gesetzeskonforme Behandlung bei Data Breach: Gesetzeskonforme Behandlung von Data Breach-Vorfällen.
- Überprüfung von Vereinbarungen: Es wird geprüft, ob alle Mitarbeiter eine Verschwiegenheitsvereinbarung unterschrieben haben und ob all jene Mitarbeiter, die Zutritt zum Hochsicherheitsbereich erhalten haben, über die Videoaufzeichnung unterrichtet wurden.

8. Technische und organisatorische Maßnahmen: Google (G Suite)

Aufgrund der Schnelllebigkeit der Technik verweisen wir aus Gründen der Praktikabilität und Aktualität sowie zum Zweck der Wahrung der Unverfälschtheit der Informationen auf die Originalsprache (Englisch) der offiziellen Quelle dieses Unterauftragsverarbeiters:

https://workspace.google.com/terms/dpa_terms.html

9. Technische und organisatorische Maßnahmen: SorryApp Inc

Aufgrund der Schnelllebigkeit der Technik verweisen wir aus Gründen der Praktikabilität und Aktualität sowie zum Zweck der Wahrung der Unverfälschtheit der Informationen auf die Originalsprache (Englisch) der offiziellen Quelle dieses Unterauftragsverarbeiters:

https://www.sorryapp.com/security-and-performance#network-and-internal-security

Stand: 23.02.2022