Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen dem lexoffice Kunden (Verantwortlicher) und Haufe Lexware GmbH & Co. KG (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 Versionen "Rechnung & Finanzen", "Buchhaltung & Finanzen", sowie "Buchhaltung & Berichte" gehören dazu im Kern die Erstellung von Ausgangsbelegen wie z.B. Angeboten, Rechnungen, Lieferscheinen etc. die Erfassung und automatische Erkennung sowie Verbuchung von Eingangsbelegen, wie z.B. Kassenbelegen oder Lieferantenrechnungen,

der Abgleich von Zahlungsvorgängen mit einem online angebundenen Bankkonto sowie die Erfassung und Speicherung von Kunden- und Lieferantendaten.

In den Versionen “Rechnung & Finanzen”, “Buchhaltung & Finanzen”, “Buchhaltung & Berichte” 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.

In den Versionen “lexoffice Local Commerce”, “lexoffice E-Commerce” und “lexoffice Commerce” ist es zusätzlich möglich, ein elektronisches Registrierkassensystem und / oder einen Online-Shop zu betreiben, weitere Online-Plattformen, wie z.B. Amazon Marketplace, anzubinden und Online-Werbung z.B. über Google Ads zu schalten.

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:

- “Rechnung & Finanzen”, “Buchhaltung & Finanzen”, “Buchhaltung & Berichte”
- “Lohn & Gehalt”
- “lexoffice Local Commerce”, “lexoffice E-Commerce” und “lexoffice Commerce”

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. 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, Rechnungsdaten, Daten zum

Zahlungsverhalten, Steuerummer / 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, IBAN/BIC, 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 2) zurückgegriffen wird, die in Ausnahmefällen außerhalb der EU/EWR ihren Sitz haben sind.

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

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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in Anlage 1).

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 Verantwortlicher 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 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 DS-GVO; 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 DS-GVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der 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 DS-GVO (Einzelheiten in Anlage 1).
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 7 dieses Vertrages.

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 oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der 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 DS-GVO 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 2 vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.
4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.
5. Der Auftragnehmer wird vom Auftraggeber ermächtigt im Namen und mit Vollmacht des Auftraggebers „Standard Contract Clauses (Processors, Beschluss der EU-Kommission vom 05.02.2010, (2010/87/EU) – genannt Standardvertrag)“ mit den Auftragsverarbeiter des Auftragsverarbeiters (Datenimporteur), die die Leistung außerhalb der EU/des EWR erbringen, und die nicht von der EU Kommission per Angemessenheitsbeschluss als sicheres Drittland deklariert wurden, für den Auftraggeber abzuschließen.
6. 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 Verantwortliche 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 Verantwortlicher von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO 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

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
    - 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 Verantwortlicher zu melden
    - die Verpflichtung, dem Verantwortlicher 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 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.

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

1. 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.
2. 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.
3. 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.
4. Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Unterzeichnung in Kraft.

Anlage 1: Technische und

organisatorische Maßnahmen

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

1. Zutrittskontrolle:
    - Gebäude allgemein:
        - Jeder Mitarbeiter 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 Mitarbeitern begleitet.
        - Die Gebäude werden videoüberwacht.
        - Ein Sicherheitsdienst überwacht die Gebäude 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 3 zu diesem Vertrag aufgeführt
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.
3. Zugriffskontrolle:
    - Zugriffsberechtigung auf lexoffice Produktivsysteme ist auf einen kleinen Kreis von Mitarbeitern (“lexoffice Systemadministratoren”) 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 3 zu diesem Vertrag.
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 DS-GVO)

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
    - Soweit dies möglich ist, werden Daten zudem nur in anonymisierter oder pseudonymisierter Form weitergeben (z.B. Google anonymizeIP)
    - Datenabrufe und Übermittlungsaktivitäten werden protokolliert
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

DS-GVO)

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 mir namentlich benannten Verantwortlichen und einer expliziten Vertreterregelung.
    - Das Notfallkonzept wird regelmäßig überprüft und aktualisiert
    - Mitarbeiter werden 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 3 zu diesem Vertrag
2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):
    - 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 DS-GVO; Art. 25 Abs. 1 DS-GVO)

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.
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.
3. Dediziertes Incident-Response-Management für lexoffice (Vgl. §3)
4. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
5. Auftragskontrolle:
    - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO 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

Anlage 2: 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	Amazon Web Services Inc. (“AWS Frankfurt”)	410 Terry Avenue North, Seattle WA 98109, United States	Hosting und Betriebsaufgaben für alle Rechnungs- und Buchhaltungsfunktionen der Versionen “Rechnung & Finanzen”, “Buchhaltung & Finanzen”, “Buchhaltung & Berichte”, “lexoffice Local Commerce”, “lexoffice Shop”, “lexoffice Commerce”
2	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
3	The Rocket Science Group LLC	675 Ponce de Leon Ave NE, Suite 5000, Atlanta,	Versand aller Arten von E-Mails mit der Applikation “Mandrill“ für alle lexoffice Versionen

		GA 30308 USA	
4	Intercom Inc.	55 2nd Street, 4th Floor, San Francisco, California, 94105, USA	Hosting und Betrieb eines Webanalyse- und Kommunikationsdienstes für alle lexoffice Versionen
5	Feldforum Ruhr, Inhaberin Karin Barkowski	Flottmann str. 56, 44625 Herne	Marktforschung für alle lexoffice Versionen
6	VersaCommerce Entwicklungs- und Betriebsgesellschaft mbH	Bödekerstraße 22, 30161 Hannover	Whitelabel POS und Shopsystem für die Versionen “lexoffice local Commerce”, “lexoffice “Shop”, lexoffice Commerce”
7	Insiders Technologies	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	LimeSurvey GmbH	Barmbeker Str. 7a, 22303 Hamburg	Online-Umfragen für alle lexoffice Versionen

10	Google Inc.	Amphitheatre Parkway, Mountain View, CA 94043, USA	Interne und externe Kommunikation über E-Mail und G-Suite Office

Anlage 3: Technische und organisatorische Maßnahmen der Unterauftragsverarbeiter

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

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

2. Technische und organisatorische Maßnahmen: Uservoice

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

1. Festlegung von bestimmten Personengruppen mit Zugangserlaubnis, dokumentiert in einem Berechtigungskonzept
2. Ausstattung des Personal mit Zugangskarten
3. Richtlinien und Verfahren für die Autorisierung und Nutzung physischer Schlüssel (Verzeichnis der Schlüsselbesitzer)
4. Richtlinien und Verfahren für Besucher und Externe (z.B.

Zugangskarten für Besucher)
5. Dokumentation/Aufzeichnung von Besuchern und Lieferanten
6. Sicherheitsmaßnahmen außerhalb der Betriebszeiten (elektrische Türöffner, Sicherheitspersonal)
7. Überwachungseinrichtungen (Alarmanlage, Bewegungsmelder) für den Außenbereich und alle sicherheitskritischen Zugänge innerhalb des Gebäudes
8. Definierte Sicherheitsbereiche mit überwachten Zugangseinrichtungen
9. Gesicherte Bereiche für Warenan- und auslieferungen
10. Gesicherte Türen (z.B. elektrische Türschließer, Leser für Zugangskarten, Alarmanlage, Überwachungskamera/Videoüberwachung, Sicherheitspersonal)
11. Dokumentation/Aufzeichnung für Zugangsgeräte/-medien (magnetische Zugangskarten, Chip-Karten, Schlüsselausgabe, Verzeichnis über Schlüsselausgabe)
12. Maßnahmen zur Objektsicherheit (z.B. Spezialverglasung, Sicherheitsschranken, Alarmanlage, Sicherheitsüberprüfung, Sicherheitspersonal)
13. Zusätzliche Sicherheitsmaßnahmen

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1. Nutzer-Berechtigungskonzepte für individuelle Nutzergruppen (bspw. beschäftigte, Besucher, Drittparteien, Subunternehmen)
2. Verwendung von Boot-Passwörtern (insbesondere Sonderzeichen, Minimallänge, Passwortwechsel beim Booten etc.)
3. Zugangskarten für Autorisierung und Zugangskontrolle
4. Sicherung von Einrichtungen der Datenverarbeitung
5. Sicherung der Netzwerkkonfiguration und des Netzwerkbetriebs,

sowohl intern als auch der Netzwerkumgebung
6. Bereitstellung und Sicherheit von Identitätsschlüsseln
7. Gesicherte Arbeitsräume
8. Abschließbare Arbeitsräume
9. Automatische funktionale oder zeitliche Sperren (z.B. Passwortsperre oder zeitgesteuertes Sperren) von Endgeräten oder Anmeldedaten
10. Richtlinien und Verfahren für die Zugangskontrolle
11. Verwendung von Benutzer-IDs oder Verschlüsselung
12. Verwendung von Einrichtungen zur Daten- und Netzwerkverschlüsselung
13. Richtlinien und Verfahren zum Umgang mit Dateien und zur Datenaufbewahrung
14. Verfahren für Tests und Freigabe von Software
15. Identifikation der zur Arbeit an Datenverarbeitungsanlagen berechtigten Personen (Passwort, Zugangscodes etc.)
16. Überprüfung, Bestätigung und Überwachung der Systeme

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1. Der Datenzugriff basiert auf einem definierten Berechtigungs- und Zugriffskonzept.
2. Automatische funktionale oder zeitliche Sperren (z.B. Passwortsperre oder zeitgesteuertes Sperren) von Endgeräten
3. Verwendung von Datenverschlüsselung
4. Richtlinien und Verfahren zur Autorisierung der Dateneingabe,

Datenveränderung und Datenlöschung
5. Regelmäßige Überprüfung und Erneuerung der Zugriffsrechte der Benutzer
6. Überprüfung der Aufzeichnungen der Benutzerzugriffe
7. Partiell beschränkte Zugriffsmöglichkeiten hinsichtlich Datenbanken und Funktionen
8. Analyse von Log-Dateien
9. Kontrolle der Zugriffsrechte (z.B. Identitätsschlüssel)

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

1. Verschlüsselung von Daten und Datenverbindungen
2. Verschlüsselung vertraulicher Daten auf Medien zur Datensicherung
3. Fest eingebaute Laufwerke
4. Gesicherte Schaltschränke
5. Gesicherte Aufbewahrung von Datenträgern innerhalb von Sicherheitsbereichen (z.B. Sicherheitsschränke, Datentresore für magnetische Datenträger)
6. Dokumentation von Software zur Suche nach und Übertragung von Daten
7. Dokumentation von Beteiligten an und Methoden zur Datenübertragung mit enthaltenen personenbezogenen Daten
8. Aufzeichnung der jeweiligen Übertragungsparameter
9. Verschlüsselter E-Mail-Versand

10. Richtlinien und Verfahren für die Vervielfältigung von Daten

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

1. Kennzeichnung eingegebener Daten
2. Organisatorische Richtlinien und Verfahren sowie Rollen und Verantwortlichkeiten bei der Datenerfassung
3. Protokollierung der Eingabe, Veränderung und Löschung personenbezogener Daten
4. Protokollierung von Zugriffsversuchen auf Daten
5. Anweisungen für Verfahren, Programme und Abläufe
6. Datenschutzverpflichtung entsprechend § 5 BDSG
7. Vertraulichkeitsvereinbarungen mit Beschäftigten und Dritten
8. Einführung von Verfahren zur Zugriffskontrolle
9. Bestimmungen über Aufbewahrungsfristen für Revision und ähnliche nachweispflichtige Fälle

6. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1. Verfahren für Daten-Backups und Daten-Wiederherstellung
2. Regelmäßige Überprüfungen von Backup-Maßnahmen und Kennzeichnung von Backup-Medien
3. Betriebskontinuität und Notfallplanung (z.B. im Fall von Schäden durch Wasser, Frost, Feuer, Explosion, Terrorbedrohungen, Flugzeugabstürzen, Erdbeben)
4. Regelmäßige Überprüfung der Notfallstromversorgung und

elektrischen Schutzeinrichtungen
5. Einwirkung von benachbarten Gebäuden
6. Identifizierung von Schwachstellen in den folgenden, aber nicht beschränkt auf diese, Bereichen:
    - Liegenschaften des Unternehmens und deren Umgebung
    - Firmengebäude und deren Infrastruktur
    - Client- und Server-Systeme
    - Daten-Netzwerke
7. Aufbewahrung von Datenträgern in feuer- und wassergeschützten Datentresoren oder Tresorräumen

7. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

1. Trennung von Kunden/Kundendaten
2. Aufgabentrennung
3. Funktionstrennung
4. Trennung von Entwicklungs-, Test- und Produktivsystemen
5. Verfahren für die Software-Entwicklung
6. Verfahren für das Software-Testing
7. Verfahrensdokumentation für personenbezogene Daten

8. Organisatorische Kontrolle

1. Richtlinien, Verfahren, Leitfaden, Arbeitsanweisungen etc.
2. Rollen und Verantwortlichkeiten
3. Kommunikationsmatrix inklusive Kontakt-Details

3. Technische und organisatorische Maßnahmen: The Rocket Science Group

Sicherheit des Datenverarbeitungszentrums

- Die Rocket Science Group versendet mehr als 17 Milliarden E-Mails pro Monat an mehr als 9 Millionen Nutzer. Wir nutzen mehrere MTAs (Mail Transfer Agents, Software/Mail-Server zum Mailversand), die sich in unterschiedlichen “Welt-Klasse”-Datenverarbeitungszentren in den USA befinden.
- Unsere Datenverarbeitungszentren verhindern den Zugang Unbefugter rund um die Uhr durch biometrische Scanner sowie weitere für Datenverarbeitungszentren übliche HighTech-Maßnahmen.
- In unseren Datenverarbeitungszentren existieren Maßnahmen zur Verhinderung von DDoS-Attacken.
- Es existiert ein dokumentierter Maßnahmenplan für den unterbrechungsfreien Betrieb “im Fall eines nuklearen Angriffs auf ein Datenverarbeitungszentrum”.

Schutz vor Datenverlust, Korruption

- Alle großen Accounts zugehörigen Datenbestände werden gesondert/dediziert verwaltet, um Korruption und Vermischung zu verhindern. Kleinere und kostenlose Accounts werden aus Performanzgründen in einer gemeinsamen großen Datenbank vorgehalten. Bei Erreichen einer bestimmten Größenordnung werden solche Accounts in gesonderte eigene Datenbanken migriert.
- Die Datenbestände der Accounts werden gespiegelt und es werden regelmäßig Back-Ups vorgenommen und extern verwahrt.

Sicherheit der Applikation

- Die Passwörter der Benutzer sind mit einem Hash versehen, sie

können auch von unseren Mitarbeitern nicht eingesehen werden. Bei Passwortverlust muss ein neues Passwort generiert werden.
- Alle Login-Seiten (sowohl Desktop als auch Mobile) verwenden das SSL-Verfahren.
- Die gesamte Anwendung ist SSL-verschlüsselt.
- Die Login-Seiten sind gegen “brute force”-Attacken geschützt.
- Login-Vorgänge via MailChimp-API sind gegen “brute force”-Attacken geschützt.
- Wir führen regelmäßig Sicherheits-/Penetrations-Tests durch und greifen dabei auf verschiedene Anbieter zurück. Die Tests beinhalten hochprofessionelle Penetrations-Tests der Server, detaillierte Tests auf Schwachstellen innerhalb der Anwendung sowie Schulungen der Mitarbeiter zum Schutz vor Manipulation/Täuschung.

Sicherheit der Mobile Apps

- Sensible Daten auf iPhone apps werden aus Sicherheitsgründen in Keychain gespeichert.
- Sensible Daten werden via SSL übertragen.
- Für entsprechende apps erfolgt eine Compliance-Prüfung durch TRUSTe.

Interne IT-Sicherheit

- Der Zutritt zu unseren Bürogebäude ist nur mit Keycard möglich und wird durchweg mit Infrarot-Kameras überwacht.

Innerbetriebliche Vorschriften und Unterweisung

- Alle neuen Mitarbeiter in Abteilungen mit Zugang zu Kundendaten (bspw. technischer Support und unsere Techniker) werden vor ihrer Einstellung auf kriminelle Vergangenheit und

Kreditwürdigkeit überprüft.

- Die Lektüre des Buches “The Art of Deception” von Kevin Mitnick ist für alle neuen Mitarbeiter Pflicht. Die Lektüre des Buches “Fatal System Error” von Joseph Menn wird empfohlen.
- Alle Mitarbeiter haben eine Datenschutzvereinbarung unterzeichnet, in der Pflichten und Verantwortlichkeiten hinsichtlich des Schutzes der Kundendaten beschrieben sind.
- Allen neuen Mitarbeiter werden Sicherheits-Richtlinien hinsichtlich der Nutzung von sozialen Medien ausgehändigt; enthalten sind auch Informationen zum Schutz vor Manipulation/Täuschung.
- Ein Verfahren zur Beendigung von Arbeitsverhältnissen (“change management”) ist etabliert.
- Um unser Unternehmen vor Verlusten unterschiedlicher Natur zu schützen, haben wir ein umfangreiches Versicherungspaket abgeschlossen. Dies wurde dahingehend ausgestaltet, dass es uns sowohl vor den üblichen Risiken einer Geschäftstätigkeit als auch speziell vor den Risiken, die unserer Geschäftstätigkeit in der Technologiebranche eigen sind, schützt. Wir haben darüber hinaus einen finanzstarken Versicherungsanbieter gewählt und beträchtliche Deckungssummen bei folgenden Versicherungen/Risiken vereinbart:
    - Sach- und Betriebsunterbrechungsversicherung
    - Betriebshaftpflichtversicherung
    - Arbeitgeberhaftpflichtversicherung
    - Geschäftswagenversicherung
    - Haftpflichtausfallversicherung
    - Internationale Sach- und Haftpflichtversicherung
    - Haftpflicht für technische Fehler und Unterlassen
    - Manager-Haftpflicht

Wir arbeiten in Übereinstimmung mit SOC II und sind zertifiziert nach

PCI DSS. Gerne stellen wir Ihnen auf Anfrage unseren vollständigen SOC II-Prüfbericht zur Verfügung.

4. Technische und organisatorische Maßnahmen: Intercom Inc.

Zutrittskontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom verhindert den Zugang Unbefugter zu den Liegenschaften des Auftragsverarbeiters.
2. Intercom verwendet Amazon Web Services, Inc. (“AWS”) , um personenbezogene Daten, die an Intercom übermittelt wurden, zu hosten und aufzubewahren. AWS setzt Intrusion-Detection-Systeme ein, um zu den Zugang zu seinen Liegenschaften zu überwachen.
3. Intercom stellt sicher, dass Unbefugte (bspw. Techniker, Reinigungspersonal) innerhalb der Liegenschaften jederzeit begleitet werden.

Zugangskontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom wendet Maßnahmen an, um den Zugang Unbefugter zu Datenverarbeitungsanlagen zu verhindern.
2. Intercom stattet jeden für den Zugang zu Datenverarbeitungsanlagen autorisierten Nutzer zu Legitimationszwecken mit einer eindeutigen ID aus.
3. Intercom implementiert ein Zwei-Faktor-Authentifizierungsverfahren für alle autorisierten Nutzer.
4. Intercom stellt sicher, dass der Zugang zu

Datenverarbeitungsanlagen nur mit Authentifizierung möglich ist, so dass Unbefugte
    1. nach Startvorgängen
    2. bei kurzfristiger Nicht-Nutzung
5. keinen Zugriff auf personenbezogene Daten erhalten.
6. Intercom stellt sicher, dass die Zugangskontrolle durch ein Authentifizierungsverfahren gestützt wird.
7. Intercom hat eine Kennwortrichtlinie implementiert, die die Nutzung von Single-Sign-On unterstützt – wenn verfügbar-, die Weitergabe von Passwörtern unterbindet und Prozesse für den Fall der Offenlegung eines Passworts definiert.
8. Intercom implementiert einen adäquaten Prozess, um einen Nutzer-Account zu deaktivieren, wenn ein Nutzer aus dem Unternehmen ausscheidet oder eine relevante Funktion nicht mehr ausübt.
9. Intercom implementiert einen adäquaten Prozess, um Administrator-Rechte anzupassen, wenn ein Administrator aus dem Unternehmen ausscheidet oder eine relevante Funktion nicht mehr ausübt.

Zugriffskontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom gewährt Zugriffsberechtigungen auf Daten nur autorisiertem Personal und nur in dem minimal erforderlichen Umfang, der für das Personal zur Erfüllung seiner Aufgaben erforderlich ist.
2. intercom stellt sicher, dass das Personal, welches Datenverarbeitungsanlagen verwendet, ausschließlich auf die Daten Zugriff hat, für die eine Zugriffsberechtigung besteht.
3. Intercom beschränkt den Zugriff auf Dateien und Programme auf

“need-to-know-basis” (Kenntnis nur wenn nötig).

Eingabekontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom hat Sicherungsmaßnahmen implementiert, welche die Datenverarbeitungsaktivitäten von Administratoren und Nutzern protokollieren.
2. Intercom gestattet ausschließlich autorisiertem Personal innerhalb ihres Aufgabengebietes, personenbezogene Daten einzugeben, zu verändern oder zu löschen.

Auftragskontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom stellt sicher, dass personenbezogene Daten nicht für andere Zwecke verwendet werden, als für die, welche auftragsgemäß bzw. auf Weisung des Auftraggebers ausgeführt werden sollen.
2. Intercom ergreift Maßnahmen um sicherzustellen, dass die Verarbeitung personenbezogener Daten sowohl durch eigenes Personal als auch durch Personal von Sub-Auftragnehmern strikt in Übereinstimmung mit den vertraglichen Vorgaben bzw. Weisungen des Auftraggebers erfolgt.

Verfügbarkeitskontrolle

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom erstellt Backups von personenbezogenen Daten, welche in speziell gesicherter Umgebung aufbewahrt werden.
2. Intercom verfügt über Notfallmaßnahmen oder Recovery-Maßnahmen.

3. Intercom hat sein Netzwerk durch Firewalls geschützt, um unbefugten Zugriff auf Systeme und Services zu verhindern.
4. Intercom stellt sicher, dass jedes zur Verarbeitung personenbezogener Daten verwendete System entsprechend den best practises und anerkannten Industriestandards hinsichtlich Systemhärtung adäquat konfiguriert und gepatched ist.

Datentrennung

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom stellt sicher, dass jede Kategorie gesammelter personenbezogener Daten ausschließlich für den Zweck verarbeitet wird, für die die Daten gesammelt wurden.

Organisatorische Erfordernisse

Intercom wendet folgende Sicherungsmaßnahmen uneingeschränkt an:

1. Intercom liegt das schriftliche Einverständnis zur Vertraulichkeit seiner Beschäftigten vor.
2. Intercom hat hinsichtlich Datenvertraulichkeit und Datensicherheit geschulte Mitarbeiter.
3. Intercom führt regelmäßige Audits durch, um die Übereinstimmung mit den Anforderungen des Datenschutzes sicherzustellen.

5. Technische und organisatorische Maßnahmen: Feldforum Ruhr

1. Organisationskontrolle:
   Datenschutz und Datensicherheit sind in der Aufbau- und Ablauforganisation von Feldforum Ruhr fest verankert.
   - Personelle Zugriffsbeschränkungen: Nur festangestellte

Mitarbeiter haben Zugriff auf personenbezogene Daten und verarbeiten im Rahmen der Projektarbeit diese. Die Datenschutzbeauftragte verfügt über Kontrollmöglichkeiten.
    - Definierter Projektablauf: Über den klar definierten Projektablauf wird dafür gesorgt, dass personenbezogene Daten nur so lange vorgehalten werden, wie sie zur Erfüllung des Projektauftrags notwendig sind.
    - Datenschutzbeauftragte: Verena Simon
    - IT-Sicherheitsbeauftragte: Heike Ackermann
2. Zutrittskontrolle:
   Unbefugte haben keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Zutritt zu den Datenverarbeitungsanlagen ist durch folgende Verfahren abgesichert:
    - Ständige Überwachung des Eingangsbereiches
    - Verweigerung des Zutritts von Geschäftsräumen gegenüber Unbefugten
    - Nach Geschäftsschluss kein Einlass in Geschäftsräume möglich
    - Kein Besucher ohne Begleitung im Hause
    - Serverräumlichkeiten sind durch zusätzliche Sicherheitstür vor unbefugtem Zutritt gesichert und ständig verschlossen
3. Zugangskontrolle:
   Feldforum Ruhr gewährleistet, dass nur autorisierte Mitarbeiter Zugang zu den Datenverarbeitungssystemen haben, mit denen personenbezogene Daten verwendet werden. Um dies zu gewährleisten, werden folgende Sicherungsmaßnahmen angewendet:
    - Zugangsberechtigung auf spezielle Nutzergruppe beschränkt
        - Adressverarbeitung nur auf besonders geschütztem Server
        - Nur autorisierte Mitarbeiter von Feldforum Ruhr

        haben Zugang zum Server, auf dem personenbezogene Daten verarbeitet werden
        - Rechtevergabe pro Projekt
    - Mehrstufiger Autorisierungsprozess
        - Rechner sind vor unbefugtem Zugriff durch mehrfache Passwortabfrage besonders geschützt (doppelte Autorisierung)
        - Erste Autorisierung erfolgt auf Betriebssystemebene am Rechner
        - Zweite Autorisierung erfolgt bei der Anmeldung am Server
        - Regelmäßige Passwortänderung
    - Anwesenheitspflicht
        - Die Mitarbeiter unterliegen einer verbindlichen Arbeitsanweisung, sich bei Verlassen des Arbeitsplatz vom System abzumelden
    - Automatische Schutzmechanismen bei Inaktivität
        - Automatische Unterbrechung des Zugangs zu sensiblen Daten nach 30 Minuten (Time Out)
        - Passwortgeschützte Bildschirmschoner nach 15 minütiger Inaktivität bei allen Mitarbeitern
    - Spezielle Sicherung für physische Medien
        - Aufbewahrung von physischen Medien bis zur Vernichtung oder Aushändigung an Auftraggeber im Tresor
4. Zugriffskontrolle:
   Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Maßnahmen zur Sicherstellung der Zugriffskontrolle:
    - Für alle DV–Systeme besteht ein aufgabenbezogenes Rollen– und Berechtigungskonzept mit entsprechenden Zugriffsrechten

    - Jeder Mitarbeiter hat nur Zugriff im Rahmen seiner Rolle/Funktion
    - Die Zuteilung der Berechtigungen erfolgt durch Vollmachten, Administratoren, deren Tätigkeit protokolliert wird
    - Alle Zugriffe werden durch das System protokolliert
5. Weitergabekontrolle:
   Es wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Maßnahmen zur Sicherstellung der Weitergabekontrolle:
    - Die elektronische Übermittlung personenbezogener Daten erfolgt entweder verschlüsselt oder über sichere Datenleitungen
    - Der physische Transport von Datenträgern erfolgt nur durch eigene Boten oder öffentliche Kurierdienste und wird protokolliert
    - Die Entsorgung von Datenträgern erfolgt durch zertifizierte Dienstleister in verschlossenen Behältnissen
    - Im Datenprotokoll werden Datenverarbeitungsschritte sowie Datenempfang und –versand festgehalten
    - Systemschnittstellen sind benutzerbezogen berechtigt und werden nur bei Notwendigkeit freigeschaltet
6. Eingabekontrolle:
   Es wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Maßnahmen zur Sicherstellung der Eingabekontrolle:
    - Dokumentation von Verarbeitungsschritten
    - Eingaben oder Veränderungen finden nicht in den Klientendatensätzen statt

    - Löschung personenbezogener Daten wird vermerkt und durch das Datenprotokoll protokolliert
7. Auftragskontrolle:
   Es wird gewährleistet, dass in Unterauftragsverhältnissen personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden. Maßnahmen zur Sicherstellung der Auftragskontrolle:
    - Sorgfältige Auswahl der Sub-Auftragnehmer
    - Vereinbarung der Datenschutzmaßnahmen in gleichem Umfang wie mit dem eigenen Auftraggeber
    - Formalisierung der Auftragserteilung
    - Kontrolle der Arbeitsergebnisse
    - Kontrolle des Auftragnehmers bezüglich Einhaltung des Vertrages
8. Verfügbarkeitskontrolle:
   Es wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Maßnahmen zur Sicherstellung der Verfügbarkeitskontrolle:
    - Sicherung der Daten
    - Zusätzliches Backup durch Sicherung mit Auslagerung bei Sicherungsabschluss. Das Backup wird täglich durch die Geschäftsleitung extern aufbewahrt.
    - Sicherung der DV–Systeme durch eine ständig verschlossene Tür mit Zugangskontrolle
    - Sicherung der DV – Systeme in einem entsprechend angepassten, abgeschlossenen Schrank.
    - Sicherung der DV–Systeme durch eine Klimaanlage mit Belüftung nach außen
    - Sicherung der Stromversorgung durch USVs
    - Kontrolle des Datenzugriffs von außen durch eine Firewall mit allen üblichen Merkmalen (Content-, Mail-, Viren/SPAM-Filter, Zugang von außen nur durch vpn möglich

mit Protokollierung der Zugriffe, Festlegung der Zugriffe von intern nach extern ebenfalls reguliert etc.)
    - Stufensystem des Virenschutz auf Server, Firewall und Laptops bzw. Desktops der Mitarbeiter
9. Datentrennung:
   Personenbezogene Daten werden nach Auftraggebern und Projekt getrennt verarbeitet. Maßnahmen zur Sicherstellung des Trennungsgebots:
    - Getrennte Ordner pro Klient und klar geregelte Zugriffsrechte, insbesondere für personenbezogene Daten
    - Die Datenbestände werden nach Abschluss des Projekts restlos gelöscht

6. Technische und organisatorische Maßnahmen: VersaCommerce

1. Maßnahmen die dazu geeignet sind Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle):
    - Gebäude allgemein:
        - Der Zugang zum Gebäude ist nur mit Sicherheitsschlüssel möglich. Nur feste Mitarbeiter erhalten diese Schlüssel.
        - Besucher müssen klingeln und werden vom Empfang zum jeweiligen Ziel begleitet und abgeholt.
        - Eingansgbereiche des Gebäudes sind Video-überwacht.
        - Eine Alarmanlage überwacht die Geschäftsräume außerhalb der Bürozeiten.
    - Rechenzentrumsräume:
        - Das Rechenzentrum von VersaCommerce befindet

sich in Frankfurt a.M. (Amazon Websphere, AWS) und ist mit allen Einrichtungen der höchsten Sicherheitsklassen ausgestattet (vgl. Technische und organisatorische Maßnahmen AWS in Anlage 3).

2. Maßnahmen die dazu geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangs- und Zugriffskontrolle):
    - Der Benutzer- und Administratorzugriff auf das VersaCommerce- 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 Vorgaben zur Passwortkomplexität.
    - Einsatz von Firewallsystemen, Virenscanner und Intrusion Detection Systemen im VersaCommerce-Firmen-Netzwerk.
    - Auf den Rechnern der VersaCommerce-Mitarbeiter sind Virenscanner installiert, die eine Malware Erkennung und einen E-Mail Filter enthalten.
    - Der Zugriff auf VersaCommerce-Serversysteme erfolgt SSH-Verschlüsselt („Public key“), der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt.
3. Maßnahmen die dazu geeignet sind, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle):
    - Datenübertragung zwischen VersaCommerce-Serversystemen erfolgt ausschließlich

innerhalb abgegrenzter 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
    - Soweit dies möglich ist, werden Daten zudem nur in anonymisierter oder pseudonymisierter Form weitergeben (z.B. Google anonymizeIP)
    - Datenabrufe und Übermittlungsaktivitäten werden protokolliert
4. Maßnahmen die dazu geeignet sind, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):
    - Sowohl Kunden- als auch Administratorzugriffe auf VersaCommerce werden automatisch protokolliert und für einige Wochen aufbewahrt.
5. Maßnahmen die dazu geeignet sind, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):
    - 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
6. Maßnahmen die dazu geeignet sind, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

(Verfügbarkeitskontrolle):
    - Es werden regelmäßig automatische Sicherungskopien und Backups aller VersaCommerce-Kundendaten erstellt.
    - Backups und Sicherungskopien sind über mehrere redundante Serversysteme und Rechenzentrumsstandorte verteilt.
    - Alle VersaCommerce-Produktivsysteme sind mehrfach redundant ausgelegt
    - Die Rechenzentren von Amazon AWS sind mit entsprechenden Schutzvorkehrungen ausgestattet (vergleiche Anlage 3)
7. Maßnahmen die dazu geeignet sind, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle):
    - Datensätze unterschiedlicher VersaCommerce-Kunden werden speziell markiert (Tenant-ID, softwareseitige Unterscheidbarkeit).
    - 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 Produktivsystem

7. 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 Kundendaten

Für die Entwicklung, den Support und die kundenspezifische Anpassung von Insiders- Lösungen kann es erforderlich sein, dass Kunden Insiders Beispieldokumente (Rechnungen, Lieferscheine, Formulare etc.) und Stammdaten zur Verfügung stellen.

Alle Kundendaten 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 zur Verfügung.

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.

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.

Insiders bietet Kunden eine cloudbasierte Dokumentverarbeitung sowie auf Wunsch auch die Dienstleistungen Scannen, Digitalisierung und Verifikation an. Hierbei handelt es sich um die Bereitstellung und

Nutzung von Software und Hardwareressourcen und der für den Zugriff erforderlichen Netzkommunikation über ein Datennetz („IaaS“ und „SaaS“-Lösungen).

Hierzu bedient sich Insiders der Dienste Dritter hinsichtlich der Bereitstellung von Rechenzentrumsleistungen sowie in Bezug auf Posteingangsbearbeitungs- und Scandienstleistungen. Solche Dritten werden als Auftragsverarbeiter für Insiders tätig und dementsprechend jeweils über eine Auftragsverarbeitungsvereinbarung verpflichtet.

Insiders wählt die Dienstleister sorgfältig aus und prüft vor der Beauftragung sowie während der Vertragslaufzeit, dass diese die nach den Vorgaben der DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben und die Regelungen aus der betreffenden Auftragsverarbeitungsvereinbarung einhalten. Die mit dem Dienstleister vereinbarten technischen und organisatorischen Maßnahmen gelten vorrangig gegenüber den in diesem Dokument genannten Maßnahmen und werden betroffenen Kunden auf Anforderungen offen gelegt.

Bei einem Wechsel eines Dienstleisters stellt Insiders sicher, dass das Sicherheitsniveau gegenüber den vereinbarten technischen und organisatorischen Maßnahmen nicht unterschritten wird.

3 Zugangskontrolle

Insiders stellt durch verschiedene Maßnahmen sicher, dass unbefugte Personen keinen Zutritt zu den Geschäftsräumen erhalten. Die Eingangsbereiche der Geschäftsräume von Insiders werden elektronisch mit Kameras überwacht. Unbefugte können somit das Unternehmen nicht unbemerkt betreten. Die Außen-Türen sind während der Betriebszeiten geschlossen und außerhalb der Betriebszeiten verschlossen. Die Zugänge zu den Geschäftsräumen von

Insiders sind mit einer Transponderschließanlage ausgestattet. Somit können Zutrittsrechte jederzeit personenbezogen entzogen oder zeitlich eingeschränkt werden. Alarmanlagen sind eingerichtet und so konfiguriert, dass die Alarmierung auch extern stattfindet.

Besucher der Geschäftsräume von Insiders werden in einer Besucherliste geführt und mit einem während des Aufenthalts sichtbar zu tragenden Besucherausweis ausgestattet. Der jeweils zuständige Insiders-Mitarbeiter holt den Besuch am Empfang ab und begleitet ihn nach Terminende wieder zum Empfang zurück.

Das externe, mit dem Colocation beauftragte Rechenzentrum verfügt über eine dedizierte Zugangskontrolle, einen Sicherheitsdienst, ein mehrstufiges Zugangskontrollsystem zum Gebäude, den Colocation Räumen und zum Rack, Videoüberwachung, sowie eine Einbruchmeldeanlage.

Die Zutrittsberechtigung zu Serverräumen ist auf befugte Mitarbeiter beschränkt.

4 Kundendaten

Der Zugang zu den Datenverarbeitungsanlagen ist durch Passworteingabe abgesichert. Die Passwortvergabe ist an die folgenden Richtlinien gekoppelt, deren Einhaltung durch technische Maßnahmen erzwungen wird:

Regelmäßige Änderung nach maximal 120 Tagen Mindestlänge von 10 Zeichen Komplexität:

- 3-aus-4-Prinzip (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen) o Divergenz zu Namen(-steilen) des Passwortnutzers

- Divergenz zu den 3 letzten Passwörtern des Passwortnutzers

Für den verschlüsselten VPN-Zugang wird eine mehrstufige Authentifizierung unter Verwendung von Token verwendet. Nach einer bestimmten Zeit der Inaktivität erfolgt eine automatische Sperrung der Rechner mit anschließendem erneutem Login. Bei Verlassen des Arbeitsplatzes ist eine manuelle Abmeldung am Rechner durchzuführen.

5 Zugriffskontrolle

Die Vergabe von Rechten auf Kundendaten erfolgt durch die Mitarbeiter der Support- Abteilung in Zusammenarbeit mit den jeweiligen Projektleitern und wird in einem Verfahrensverzeichnis dokumentiert.

Mitarbeiter der Abteilungen Support und Technische Administration haben Zugriff auf alle Kundendaten-Verzeichnisse. Zugriffe auf Kundendaten werden auf dem Kunden-Fileserver dokumentiert. Im Rahmen regelmäßiger Kontrollen und Abstimmungen ermitteln die beteiligten Support- und Administrationsmitarbeiter, ob bestehende Rechte weiter benötigt werden oder eingeschränkt bzw. entzogen werden müssen.

Diese Kontrollen erfolgen regelmäßig halbjährlich, bei Personaleinstellungen und –Abgängen, bei Änderungen in der Zusammensetzung eines Projektteams sowie, in Absprache mit dem Kunden, zu vertraglich festgelegten Terminen.

6 Weitergabekontrolle

Arbeitsrechtlich unterliegen alle Insiders-Mitarbeiter einer vorgegebenen Routine im Umgang mit Daten und den zur Verfügung stehenden IT-Strukturen. Die Weitergabe von Daten durch Mitarbeiter an Dritte ist nur dann zulässig, wenn diese Weitergabe mit Zustimmung

des Kunden erfolgt. Ohne diese Zustimmung erfolgt keine Weitergabe von Daten.

Technisch wird sichergestellt, dass Daten bei einer Übertragung nicht unbefugt gelesen, abgefangen oder auf sonstige Weise von unbefugten Dritten zur Kenntnis genommen werden können, indem die Übertragung nur als verschlüsselte Anlage zu einer E-Mail oder über HTTPS erfolgt.

Dieses Vorgehen wird jeweils durch die Fachvorgesetzten und die Mitarbeiter des Supports sowie der Technischen Administration kontrolliert.

7 Eingabekontrolle

Soweit Insiders in produktiven Systemen mit personenbezogenen Daten arbeitet, werden Veränderungen an und in Dokumenten und an Datenbanken oder sonstigen Datensätzen protokolliert. Dokumente früherer Entwicklungsstadien werden gespeichert und verfügbar gehalten. Die Nachverfolgung, ob Veränderungen vorgenommen wurden und wer welche Änderung herbeigeführt hat, ist technisch gewährleistet.

8 Auftragskontrolle

Insiders verarbeitet datenschutzrechtlich relevante Vorgänge ausschließlich im Rahmen der bestehenden vertraglichen Vorgaben des jeweiligen Kunden. Insiders setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Einhaltung der Vorgaben wird regelmäßig kontrolliert.

9 Verfügbarkeitskontrolle

Die in Bezug auf die Erstellung von Backups dargestellten Maßnahmen

finden im Auftragsverhältnis nur insoweit Anwendung als mit dem jeweiligen Kunden keine abweichenden Backup-Regelungen getroffen sind. Sollte der Kunde eine jederzeit mögliche vollständige Löschbarkeit wünschen, werden die Daten dieses Kunden vom Backup ausgenommen.

Datensicherungen werden täglich durchgeführt und separat aufbewahrt. Die verwendeten Backup-Systeme für die Server befinden sich räumlich getrennt vom externen Rechenzentrum. Das gesamte System nebst allen projekt- und personenbezogenen Daten kann nach einem Ausfall zeitnah und selbst im Falle eines Totalausfall innerhalb von einigen Tagen voll einsatzbereit wiederhergestellt werden. Ein Zugriff auf die im externen, mit dem Colocation beauftragten Rechenzentrum betriebenen Systeme ist auch während der Wiederherstellungsphase möglich, soweit die für den Zugriff erforderliche Infrastruktur zur Verfügung steht.

Das zentrale Backup-System besteht aus redundanten Backup-Servern mit jeweils lokal angeschlossenen LTO-5 Tape Libraries. Als Backup-Strategien werden sowohl Tape-Backups als auch Disk-to-Disk-Backups verwendet.

Backups erfolgen nach einem für die verschiedenen Datensysteme nach Relevanz abgestuften Backup-System. Die Einstufung der verschiedenen Server, Verzeichnisse und Intervalle sowie die Benennung der verantwortlichen Person werden der Technischen Administration durch Festlegungen der Fachverantwortlichen, des IT-Sicherheitsbeauftragten und der Geschäftsleitung vorgegeben.

Eine Vielzahl von Kunden-Test- und -Entwicklungssystemen werden auf virtuellen Maschinen vorgehalten. Hierzu stehen gespiegelte VMware-Umgebungen zur Verfügung.

Insiders nutzt ein Sicherheits- und Monitoring-System, das zahlreiche Überwachungs- möglichkeiten, wie Raumüberwachung, Überwachung von Umgebungstemperaturen sowie Rauch- und Feuermeldungen, bietet. Die zentralen Räume – insbesondere die Serverräume, die Flure und auch die Besprechungsräume – sind mit Rauchmeldern ausgestattet. Das Rechenzentrum verfügt über eine unterbrechungsfreie Stromversorgung mit redundanter Gebäudezuführung, einen Schutz vor Spannungsschwankungen im öffentlichen Stromnetz, eine Notstromversorgung über USV und Dieselgenerator, eine redundante Kälte- und Klimaversorgung, Brandmeldesysteme mit Früherkennung, eine Gas-Löschanlage, Videoüberwachung und eine Einbruchmeldeanlage.

Die Entsorgung von Daten erfolgt gemäß den jeweiligen vertraglichen Vorgaben. Neben der dauerhaften Löschung der Dateien auf einem Datenträger erfolgt die datenschutzgerechte Entsorgung des Datenträgers oder die Übergabe des Datenträgers an den Insiders-Kunden.

Unterlagen und andere körperlich vorhandene Daten werden gemäß den jeweiligen vertraglichen Vorgaben entsorgt.

Sofern eine Entsorgung durch Insiders erfolgt, werden zu entsorgende Unterlagen und Datenträger einem zertifizierten Datenvernichtungsunternehmen zur Vernichtung nach DIN 66399, mindestens gemäß Schutzklasse 2 sowie den Sicherheitsstufen P-4/T-4 übergeben.

10 Trennungskontrolle

Für die Verwaltung von Kundendaten stehen dedizierte File- und Datenbankserver zur Verfügung. Diese Server werden in einem speziellen Kunden-VLAN betrieben und verfügen über eigene Benutzerverwaltungen. Kundendaten werden jeweils vertrags- und

projekt- bezogen getrennt und in verschiedenen Datenbanken gespeichert. Die Vergabe der Zugriffsrechte erfolgt wie oben beschrieben, so dass ein interner Zugriff auf Projektdaten nur den Projektmitarbeitern und auch diesen nur im Rahmen der Vorgaben möglich ist. Ein externer Zugriff ist nicht vorgesehen.

11 Verfahren zur regelmäßigen Überprüfung der Wirksamkeit

Insiders kontrolliert in regelmäßigen Zeitabständen (mindestens jährlich) die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen. Hierzu befassen sich definierte verantwortliche Stellen mindestens mit den in einer Verfahrensbeschreibung für solche Überprüfungen aufgeführten Leitfragen, dokumentieren die Ergebnisse, leiten ggf. Maßnahmen zur Verbesserung ein und verfolgen die Umsetzung derselben. Wenn sich im Rahmen einer solchen Überprüfung ergibt, dass sich Risiken geändert haben, fließen diese Erkenntnisse in die Bewertung ein und lösen bei Bedarf Anpassungsmaßnahmen aus.

8. Technische und organisatorische Maßnahmen: B+S AG

1. Vertraulichkeit

Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Elektronisches / Biometrisches Zutrittskontrollsystem
- Schlüssel und Türsicherung
- Alarmanlagen
- Videoüberwachung
- Bewegungsmelder

- Perimeter Absicherung

Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Einrichtung eines Benutzerstammsatzes pro User
- Kennwort- / Passwortschutz gemäß den Windows Sicherheitsrichtlinien
- Firewall / mehrschichtige IPS
- Antiviren Software
- Automatischer Sperrmechanismen

Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung im bestehenden Ticket System:

- Differenzierte Berechtigungen (Profile, Rollen, Gruppen)
- Protokollierung
- Prüfungsprozesse der vergebenen Berechtigungen
- Benutzererkennung mit Passwort und oder OTP
- Gesicherte Schnittstellen (Endpoint Security)
- Datenträgerverwaltung

Pseudonymisierung/Verschlüsselung

Zur Sicherstellung der Vertraulichkeit der Daten.

- Verschlüsselung von Daten

- Verschlüsselung von externen Backups
- Verschlüsselung von Übermittlungen
- Automatisierter Verschlüsselte Mailverkehr (sofern vom Kunden unterstützt)
- Verschlüsselte Tunnelverbindung – VPN (sofern vom Kunden gewünscht)

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- „Interne Mandantenfähigkeit“ / Zweckbindung des Ticketsystems
- Funktionstrennungen

2. Integrität

Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselte Tunnelverbindung – VPN (sofern vom Kunden gewünscht)
- Automatisierter Verschlüsselte Mailverkehr (sofern vom Kunden angenommen)
- Protokollierung
- Transportsicherung bei Auslagerung von Backups
- Audits von externen Backups
- Verschlüsselung von externen Backups
- Verschlüsselung von Übermittlungen

Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Zentralisierte Protokollierung
- Dokumentation der Eingabeverfahren

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Brandschutzeinrichtungen
- Wasserschutzeinrichtungen im Serverbereich
- Tägliche Bandsicherung mit Datenhaltung auf 3 Standorten
- SAN (RAID-10; RAID-5)
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung der verschlüsselten Sicherungen in einem Banksafe
- Virenschutz / Firewall
- Notfallplan (Regelmäßige DRP-Tests)
- Notfallübungen

4. Verfahren zur regelmäßigen Überprüfung Bewertung und Evaluierung

Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsdatenverarbeitung)
- Dokumentation der Zuständigkeiten

- Auftragsverarbeitungsvereinbarungen mit Dienstleistern

Allgemeine Verfahren

- Datenschutzmanagementsystem
- Informationssicherheitsmanagementsystem
- Regelmäßige Mitarbeiter-Schulungen
- Verpflichtung auf Datengeheimnis
- Prüfung und Dokumentation von Sicherheitsmaßnahmen
- Trennung von Produktiv und Testsystemen

9. Technische und organisatorische Maßnahmen: LimeSurvey GmbH

Zur Gewährleistung des Auftragnehmers zur gesetzesmäßigen Verarbeitung von personenbezogenen Daten im Auftrag, werden folgende technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO eingehalten:

I | Vertraulichkeit

I.1 | Zutrittskontrolle (z.B. für Gebäude und Räume, aber auch Schränke)

Mindestmaßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

I.1.a | Rechenzentrum

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren

- Videoüberwachung an den Ein- und Ausgängen

I.1.b | Büroräume (LimeSurvey GmbH)

- Besucher können Büroräume nicht unbeaufsichtigt betreten.
- Eingangstüren zu Büroräumen sind besonders widerstandsfähig und aus Metall.
- Alle Türen sind mit Sicherheitsschlössern ausgestattet.
- Sichere Schließanlage mit Transponderkarten
- Individuell abschließbare Schränke

I.2 | Zugangskontrolle (keine unbefugte Systembenutzung, z.B. unerlaubtes Hochfahren oder unbefugte Anmeldung in Systemen)

Mindestmaßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

I.2.a | Rechenzentrum

- Die Passwörter für die bereitgestellten dedizierten Server werden vom Auftraggeber LimeSurvey GmbH nach erstmaliger Inbetriebnahme selbst geändert und sind dem Auftragnehmer (Rechenzentrum) nicht bekannt.

I.2.b | Software (LimeSurvey)

- Passwörter in LimeSurvey werden ausschließlich durch Auftraggeber festgelegt.
- Passwörter werden nicht direkt gespeichert, sondern nur ein Salted SHA-256 Hash

I.2.d | Büroräume/Mitarbeiter (LimeSurvey GmbH)

- Die Authentifizierung gegenüber dem Betriebssystem und den Anwendungen erfolgt per individueller Benutzerkennung und Passwort
- Automatische Sperre durch Bildschirmschoner mit Passworteingabe nach 5 Minuten Inaktivität. Die Mitarbeiter sind außerdem angewiesen, den Arbeitsplatz-Rechner beim Verlassen des Raumes zu sperren.
- Die Mitarbeiter sind angewiesen, Passwörter geheim zu halten und bei Verdacht auf Kompromittierung zu ändern
- An die Passwörter werden folgende Mindestanforderungen gestellt:
    - Das Passwort muss mindestens 10 Zeichen haben.
    - Das Passwort muss Zeichen aus mindestens drei der folgenden vier Gruppen enthalten: a-z, A-Z, 0-9, sonstige druckbare ASCII-Zeichen.
    - Um die Gefahr zu reduzieren, dass Passwörter erraten werden, dürfen keine Trivial-Passwörter verwendet werden (trivial wäre ein Wort aus einem Lexikon, Name oder Vorname, die Benutzerkennung, das Geburtsdatum, das Kfz-Kennzeichen, die Telefonnummer oder andere Angaben aus dem persönlichen Umfeld des Benutzers, die auch anderen Personen bekannt sein können).
- Mitarbeiter sind angewiesen ihre Rechner-Festplatten komplett zu verschlüsseln, sowohl für Desktop-PCs als auch für mobile PCs (Notebooks, Laptops).
- Mitarbeiter ist es untersagt mobile Datenträger ohne vorherige Absprache zu verwenden oder betriebsfremde Software zu installieren.

I.3 | Zugriffskontrolle (Anwendungen ausführen, unerlaubte Tätigkeiten in IT-Systemen und Zugriffe auf Daten, Applikationen und Schnittstellen verhindern)

Mindestmaßnahmen, die gewährleisten, dass die zur Benutzung eines

Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

I.3.a | Systemadministration (LimeSurvey GmbH)

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Vollständige und ordnungsgemäße Löschung/ Vernichtung von Datenträgern vor einer anderweitigen Verwendung oder Weitergabe
- Verwaltung der System- und Benutzer-Rechte durch definierte Systemadministratoren

I.3.b | Büroräume/Mitarbeiter (LimeSurvey GmbH)

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Die Datenverarbeitungssysteme (Internet, E-Mail, Serversysteme, etc ...) werden ausschließlich für berufliche Belange genutzt.
- Inhalte/Daten dürfen nur dann auf einem Server oder dem eigenen PC gespeichert werden, wenn dies für berufliche Belange erforderlich ist. Nicht mehr benötigte Inhalte/Daten sind zu löschen.
- Regelmäßige Überprüfung und Aktualisierung der Berechtigungen einschließlich Sperrung von z.B. ausgeschiedenen Mitarbeitern
- Zugriffsprotokollierung und Auswertung findet mindestens jährlich statt
- Überprüfung und Dokumentation, an welche Stellen personenbezogene Daten übermittelt wurden (Übertragungskontrolle)
- Laufwerksspezifischer Zugriff
- Vollständige und ordnungsgemäße Löschung/ Vernichtung von

Datenträgern vor einer anderweitigen Verwendung oder Weitergabe
- Einsatz von Aktenvernichtern einer angemessen hohen Sicherheitsstufe
- Verbot von Bring-Your-Own-Device

I.4 | Trennungskontrolle

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken und für verschiedene Auftraggeber erhobene Daten wurden, getrennt verarbeitet werden:

- Logische Mandantentrennung (softwareseitig)
- Festlegung von individuellen Datenbankrechten
- Getrennte Datenbank und Datenbank-Benutzer mit Passwort für jeden Auftraggeber
- Mit der Vertragssoftware erhobene Daten werden nur vom Auftraggeber bzw. zu dem im Vertrag definierten Zweck verwendet.

I.5 | Pseudonymisierung

Die Verarbeitung erfolgt, soweit möglich, in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer natürlichen Person zuzuordnen sind.

I.5.a | LimeSurvey Webseite

Die Erfassung von IP-Adressen wird in der Systemadministration vermieden und erfasste IP-Adresse werden durch Kürzung anonymisiert.

I.5.b | LimeSurvey SaaS

Möglichkeit der Anonymisierung/Pseudonymisierung durch den Auftraggeber

II | Integrität

II.1 | Weitergabekontrolle

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Date bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

II.1.a | Rechenzentrum (Hetzner)

- Alle Mitarbeiter sind in Sachen Datenschutz geschult/belehrt worden.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

II.1.b | Software (LimeSurvey)

- SSL Verbindungen immer verfügbar (standardmäßig aktiviert, kann von Auftraggeber jederzeit selbst innerhalb der Software aktiviert/deaktiviert werden)

II.1.c | Büroräume/Mitarbeiter (LimeSurvey GmbH)

- Die Nutzung von mobilen Datenträgern ist grundsätzlich untersagt.
- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.
- Die E-Mail-Kommunikation und der Zugriff auf Dokumente der

Mitarbeiter von LimeSurvey GmbH werden durch
- Verschlüsselung und Firewalls geschützt.
- Verwendung von VPN bei mobilem Zugriff auf das Firmennetzwerk

II.2 | Eingabekontrolle (Nachvollziehbarkeit, Dokumentation)

Mindestmaßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

II.2.a | Software (LimeSurvey)

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten durch Auftraggeber
- Möglichkeit der Aktivierung eines Audit-Logs durch den Auftraggeber um Datenänderungen zu protokollieren

II.2.b | Büroräume/Mitarbeiter (LimeSurvey GmbH)

- Alle Mitarbeiter unterzeichnen eine Verschwiegenheitsklausel, die auch den Auftraggeber über die Beschäftigung hinaus schützt.
- Alle Mitarbeiter des Auftragnehmers können nur auf solche Daten zugreifen, die für ihre Arbeit erforderlich sind.
- Mitarbeiter dürfen nur auf Daten eines Kunden im Rahmen fest definierter Regeln zugreifen

III | Verfügbarkeit

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, gegen technische Störungen durch das Versagen der Betriebs-/Anwendungssoftware, vor

fahrlässigen/vorsätzlichen Handlungen, vor schadenstiftender Software geschützt sind:

III.1 | Rechenzentrum

- Einsatz unterbrechungsfreier Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Das Brandfrühesterkennungssystem ist mit der Brandmeldezentrale der örtlichen Feuerwehr verbunden
- Klimaanlage in Serverräumen

III.2 | Systemadministration (LimeSurvey Professional)

- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall
- Regelmäßige Aktualisierung aller Softwarekomponenten, mindestens alle 7 Tage.
- Backup- & Recoverykonzept:
    - Generelle Datensicherung für alle Benutzerdateien (Bilder, Designvorlagen usw.) werden alle 24 Stunden inkrementell (also nur Änderungen) gesichert.
    - Eine Hauptsicherung wird alle 7 Tage durchgeführt. Es werden maximal 2 Hauptsicherungen vorgehalten.
    - Die Daten in der Benutzerdatenbank werden alle 24 Stunden komplett gesichert. Es werden die letzten 7 Tage täglich vorgehalten; wöchentliche Sicherungen werden für 4 Wochen vorgehalten.
    - Alle Daten werden bei der Sicherung verschlüsselt und auf einem speziellen externen Datensystem gespeichert (im gleichen Rechenzentrum).

    - Alle Server sind generell mit Raid 1 Festplatten-Systemen ausgestattet, bei einem Festplattenausfall läuft nach einer kurzen Betriebsunterbrechung (Neustart des Servers) die Software auf einer Festplatte weiter. In der Regel wird die defekte Festplatte innerhalb von 24 Stunden getauscht, so dass dann wieder die volle Sicherheit gegeben ist.

IV | Kontrolle (Sonstige, Überprüfung, Bewertung und Evaluierung)

Mindestmaßnahmen, die sicherstellen, dass die Maßnahmen geeignet sind, die Sicherheit zu gewährleisten und den Belastungen standhalten, möglichst mit festen Mindestzeitintervallen

IV.1 | Generell

- Gemäß den rechtlichen Vorgaben wird ein externer Datenschutzbeauftragter beschäftigt.
- Angestellte werden in Sachen Datenschutz geschult

IV.2 | Rechenzentrum (Hetzner)

- Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.

IV.3 | LimeSurvey

- Logische Mandantentrennung (softwareseitig)
- Festlegung von individuellen Datenbankrechten
- Getrennte Datenbank und Datenbank-Benutzer mit Passwort für jeden Auftraggeber
- Mit der Vertragssoftware erhobene Daten werden nur vom

Auftraggeber bzw. zu dem im Vertrag definierten Zweck verwendet.

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

1. Datenverarbeitungsanlagen und Netzwerksicherheit

(a) Datenverarbeitungsanlagen

Infrastruktur. Google unterhält geographisch verteilte Rechenzentren. Google speichert alle produktiven Daten in physisch gesicherten Rechenzentren.

Redundanz. Die Infrastruktursysteme wurden dahingehend konzipiert, einzelne Fehlerquellen zu eliminieren und die Auswirkungen von zu erwartenden Umweltrisiken zu minimieren. Zweifache Schaltkreise, Schalter, Netzwerke oder andere notwendige Geräte tragen dazu bei, diese Redundanz bereitzustellen. Die Services ermöglichen es Google, bestimmte Arten der präventiven und korrektiven Wartung unterbrechungsfrei durchzuführen. Alle Anlagen und Einrichtungen verfügen über dokumentierte vorbeugende Wartungsverfahren, die den Prozess und die Häufigkeit der Leistungserbringung gemäß den Hersteller- oder internen Spezifikationen detailliert beschreiben. Die vorbeugende und korrektive Wartung der Rechenzentrumsanlagen wird nach einem standardisierten Änderungsprozess gemäß den dokumentierten Verfahren geplant.

Stromversorgung. Die Stromversorgungssysteme für Rechenzentren sind so konzipiert, dass sie redundant sind und gewartet werden können, ohne den kontinuierlichen Betrieb zu beeinträchtigen, 24

Stunden am Tag und 7 Tage die Woche. In den meisten Fällen wird für kritische Infrastrukturkomponenten im Rechenzentrum sowohl eine primäre als auch eine alternative Stromquelle mit jeweils gleicher Kapazität bereitgestellt. Notstrom wird durch verschiedene Mechanismen wie bspw. batteriegestützte unterbrechungsfreie Stromversorgungen (USV) zur Verfügung gestellt, die einen durchweg zuverlässigen Leistungsschutz während Versorgungsspannungsabfällen, Stromausfällen, Überspannung, Unterspannung und außerhalb der Toleranz liegenden Frequenzbedingungen liefern. Wenn die Netzstromversorgung unterbrochen wird, ist die Notstromversorgung so ausgelegt, dass das Rechenzentrum bei voller Auslastung für bis zu 10 Minuten mit Strom versorgt wird, bis die Dieselgeneratorsysteme die Stromversorgung übernehmen. Die Dieselgeneratoren sind in der Lage, innerhalb von Sekunden automatisch hochzufahren, um genügend Notstrom zu liefern, um das Rechenzentrum typischerweise über einen Zeitraum von mehreren Tagen mit voller Kapazität zu betreiben.

Serverbetriebssysteme. Die Server von Google verwenden eine Linux-basierte Implementierung, die auf die Anwendungsumgebung hin angepasst wurde. Daten werden unter Verwendung proprietärer Algorithmen gespeichert, um die Datensicherheit und -redundanz zu erhöhen. Google verwendet einen Code-Review-Prozess, um die Sicherheit des Codes, der für die Bereitstellung der Services verwendet wird, zu erhöhen und die Sicherheit in produktiven Umgebungen zu verbessern.

Betriebskontinuität. Google repliziert Daten über mehrere Systeme hinweg zwecks Schutz vor versehentlicher Zerstörung oder Verlust. Google hat Verfahren zur Betriebskontinuität/Notfallpläne entwickelt und überprüft und testet diese regelmäßig.

(b) Netzwerke und Datenübertragung.

Datenübertragung. Die Rechenzentren sind üblicherweise über private Hochgeschwindigkeits-Verbindungen verbunden, um einen sicheren und schnellen Datentransfer zwischen ihnen zu gewährleisten. Dies soll gewährleisten, dass Daten während der elektronischen Übertragung oder des Transports oder während der Aufzeichnung auf Datenträger weder gelesen, kopiert, geändert oder entfernt werden. Google überträgt Daten über Internetstandardprotokolle.

Angriffe von außen. Google verwendet mehrere Schichten von Netzwerkgeräten und Systeme zur Eindringungserkennung, um sich vor Angriffen von außen zu schützen. Google berücksichtigt potenzielle Angriffsvektoren und integriert geeignete speziell entwickelte Technologien in nach außen gerichteten Systemen.

Eindringungserkennung. Die Eindringungserkennung soll Einblick in laufende Angriffsaktivitäten geben und ausreichende Informationen bereitstellen, um auf entsprechende Vorfälle zu reagieren. Die Eindringungserkennung von Google beinhaltet:

1. Engmaschige Kontrollen hinsichtlich Größe und Art möglicher Angriffsflächen durch vorbeugende Maßnahmen;
2. Einsatz intelligenter Erkennungsmechanismen an Dateneingabestellen; und
3. Einsatz von Technologien, die bestimmte gefährliche Situationen automatisch entschärfen.

Reaktion auf sicherheitsrelevante Vorfälle. Google überwacht über eine Vielzahl an Kommunikationskanälen das Auftreten von sicherheitsrelevanten Vorfällen und das Sicherheitspersonal von Google reagiert umgehend auf bekannte Vorfälle.

Verschlüsselungstechnologien. Google stellt HTTPS-Verschlüsselung (auch als SSL oder TLS bezeichnet) zur Verfügung.

2. Zugangskontrollen

(a) Zugang zu Liegenschaften.

Sicherheitskontrollen der Rechenzentren. Die Rechenzentren von Google werden vor Ort 24 Stunden am Tag, 7 Tage die Woche überwacht. Das Sicherheitspersonal vor Ort beobachtet mittels Videoüberwachungsssystemen und überwacht alle Alarmsysteme. Außerdem werden innerhalb und außerhalb der Rechenzentren regelmäßig Kontrollgänge durchgeführt.

Zutrittskontrollen. Google hat festgelegte Zutrittsverfahren für den physischen Zutritt zu den Rechenzentren. Die Rechenzentren sind in Einrichtungen untergebracht, die einen Zutritt nur mit elektronischen Zugangskarten ermöglichen, mit Alarmsystem für das Sicherheitspersonal vor Ort. Alle in das Rechenzentrum Eintretenden müssen sich ausweisen und gegenüber dem Sicherheitspersonal identifizieren. Nur autorisierte Mitarbeiter, Auftragnehmer und Besucher erhalten Zutritt zu den Rechenzentren. Nur autorisierten Mitarbeitern und Auftragnehmern ist es gestattet, elektronische Zugangskarten für diese Einrichtungen zu beantragen. Anträge für elektronische Zugangskarten müssen per E-Mail erfolgen und erfordern die Genehmigung des Vorgesetzten des Beantragenden sowie des Direktors des Rechenzentrums. Alle anderen Besucher, die einen temporären Zutritt zum Rechenzentrum benötigen, müssen: (i) vorab von den Verantwortlichen des Rechenzentrums eine Genehmigung für das spezifische Rechenzentrum und die internen Bereiche erhalten, die sie besuchen möchten; (ii) sich beim Sicherheitspersonal vor Ort anmelden (iii) und eine genehmigte Zutrittserlaubnis des Rechenzentrums aufweisen können, in der die entsprechende Person

als genehmigt identifiziert wird.

Sicherheitseinrichtungen im Rechenzentrum. Die Rechenzentren von Google verwenden eine elektronische Zugangskarte und ein biometrisches Zutrittskontrollsystem, welches mit einem Systemalarm verbunden ist. Das Zutrittskontrollsystem überwacht und zeichnet die Daten der elektronischen Zugangskarte jeder Person auf, wenn diese Eingangstüren, Versand- und Empfangsbereiche und andere kritische Bereiche passieren. Nicht autorisierte Aktivitäten und fehlgeschlagene Zutrittsversuche werden vom Zutrittssteuerungssystem protokolliert und gegebenenfalls untersucht. Der autorisierte Zutritt im gesamten Geschäftsbetrieb und in den Rechenzentren ist in Zonen aufgeteilt und gemäß der Verantwortlichkeit des einzelnen Mitarbeiters beschränkt. Die Feuerschutztüren in den Rechenzentren sind mit Alarmanlagen ausgestattet. Videoüberwachungssysteme sind sowohl innerhalb als auch außerhalb der Rechenzentren in Betrieb. Die Kameras wurden so positioniert, dass sie strategische Bereiche abdecken, unter anderem die Umgebung, Türen zum Gebäude des Rechenzentrums und den Versand/Empfang. Sicherheitsmitarbeiter vor Ort verwalten die Videoüberwachungs-, Aufzeichnungs- und Kontrollgeräte. Gesicherte Leitungen in den Rechenzentren verbinden die Videoüberwachungs-Geräte. Kameras zeichnen 24 Stunden am Tag, 7 Tage die Woche auf digitale Videorekorder vor Ort auf. Die Aufzeichnungen werden je nach Aktivität für bis zu 90 Tage aufbewahrt.

(b) Zugangskontrolle.

Organisation des Sicherheitspersonals. Google verfügt über und hält aufrecht eine Sicherheitsrichtlinie für sein Personal sowie verpflichtende Sicherheitsschulungen als Teil des Schulungspakets für seine Mitarbeiter. Das Sicherheitspersonal von Google ist für die laufende Überwachung der Sicherheitsinfrastruktur von Google, die Überprüfung der Dienste und die Reaktion auf Sicherheitsvorfälle

verantwortlich.

Zugriffskontrolle und Rechteverwaltung. Die Administratoren und Endbenutzer bei Google müssen sich über ein zentrales Authentifizierungssystem oder über ein Single-Sign-On-System authentifizieren, um die Dienste nutzen zu können. Jede Anwendung überprüft die Anmeldeinformationen vor der Anzeige von Daten für autorisierte Endbenutzer oder autorisierte Administratoren.

Interne Datenzugriffsprozesse und -richtlinien – Zugriffsrichtlinien. Die internen Datenzugriffsprozesse und -richtlinien von Google verhindern, dass unbefugte Personen und / oder Systeme auf Systeme zur Verarbeitung personenbezogener Daten zugreifen. Google gestaltet seine Systeme so, dass (i) nur berechtigten Personen Zugriff auf die Daten gewährt wird, auf die sie zugreifen dürfen; und (ii) sichergestellt ist, dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Aufzeichnung nicht ohne Genehmigung gelesen, kopiert, geändert oder entfernt werden können. Die Systeme sind so konzipiert, dass sie jeden unangemessenen Zugriff erkennen können. Google verwendet ein zentralisiertes Zugriffsverwaltungssystem, um den Zugang der Mitarbeiter zu den Produktionsservern zu kontrollieren, und gewährt nur einer begrenzten Anzahl von autorisiertem Personal Zugang. LDAP, Kerberos und ein proprietäres System, das RSA-Schlüssel verwendet, sind so konzipiert, dass sie Google die Gestaltung sicherer und flexibler Zugriffsmechanismen ermöglichen. Diese Mechanismen dienen dazu, dass auf Site-Hosts, Logs, Daten und Konfigurationsinformationen nur mit Genehmigung zugegriffen werden kann. Google verwendet eindeutige Benutzer-IDs und starke Kennwörter, Zwei-Faktor-Authentifizierung und sorgfältig überwachte Zugriffslisten, um das Risiko der unbefugten Nutzung eines Benutzerkontos zu minimieren. Die Gewährung oder Änderung von Zugriffsrechten erfolgt gemäß: den tätigkeitsbezogenen Verantwortlichkeiten; tätigkeitsbezogenen Anforderungen zur

Ausführung bestimmter Aufgaben; der “need-to-know-basis” (Kenntnis nur wenn nötig); und muss den internen Datenzugriffsrichtlinien und Schulungen von Google entsprechen. Genehmigungen werden von Workflow-Tools verwaltet, die Prüfprotokolle aller Änderungen verwalten. Der Zugriff auf Systeme wird protokolliert, um einen Prüfpfad für die Verantwortlichkeit zu erstellen. Wo Passwörter für die Authentifizierung verwendet werden (z. B. beim Anmelden an Workstations), werden Passwortrichtlinien implementiert, die mindestens den Industriestandards entsprechen. Zu diesen Standards gehören ein Ablaufdatum für ein Kennwort, Einschränkungen bei der Wiederverwendung von Kennwörtern und ausreichende Kennwortstärke. Für den Zugriff auf äußerst vertrauliche Informationen (z. B. Kreditkartendaten) verwendet Google Hardware-Token.

3. Daten.

(a) Datenspeicherung, Datentrennung und Authentifizierung.

Google speichert Daten in einer mandantenfähigen Umgebung auf eigenen Servern. Daten, die Datenbank des Dienstes und die Dateisystemarchitektur werden zwischen mehreren geografisch verteilten Rechenzentren repliziert. Google trennt die Daten logisch je Endbenutzer auf der Anwendungsebene. Google trennt außerdem die Daten des Datenexporteurs logisch und der Datenexporteur erhält die Kontrolle über spezifische Datenfreigaberichtlinien. Google trennt die Daten des Datenexporteurs, einschließlich der Daten verschiedener Endbenutzer, logisch voneinander, und Daten für einen authentifizierten Endbenutzer werden keinem anderen Endbenutzer angezeigt (es sei denn, der frühere Endbenutzer oder Administrator erlaubt die gemeinsame Nutzung der Daten). Ein zentrales Authentifizierungssystem wird für alle Dienste verwendet, um die Sicherheit der Daten zu erhöhen. Der Datenexporteur erhält die Kontrolle über bestimmte Datenfreigaberichtlinien. Diese Richtlinien ermöglichen es dem Datenexporteur, in Übereinstimmung mit der

Funktionalität der Dienste die Einstellungen für die Produktfreigabe festzulegen, die für Endbenutzer für bestimmte Zwecke gelten. Der Datenexporteur kann bestimmte Protokollierungsfunktionen verwenden, die Google über die Dienste, Produkte und APIs bereitstellen kann. Der Datenexporteur stimmt zu, dass seine Verwendung der API den Nutzungsbedingungen der API entspricht.

(b) Außer Betrieb genommene Datenträger und Richtlinien zur Löschung von Datenträger

Bei bestimmten Datenträgern können Leistungsprobleme, Fehler oder Hardwarefehler auftreten, die dazu führen, dass sie außer Betrieb genommen werden („Außer Betrieb genommene Datenträger"). Jeder außer Betrieb genommene Datenträger unterliegt einer Reihe von Datenvernichtungsprozessen (die „Richtlinie zur Datenträgerlöschung"), bevor er die Räumlichkeiten von Google entweder zur Wiederverwendung oder zur Zerstörung verlässt. Außer Betrieb genommene Festplatten werden in einem mehrstufigen Prozess gelöscht und ihre Löschung durch mindestens zwei unabhängige Prüfer verifiziert. Die erfolgte Löschung wird mit der Seriennummer der außer Betrieb genommenen Festplatte zwecks Nachverfolgung protokolliert. Schließlich wird die gelöschte und außer Betrieb genommene Platte für die Wiederverwendung und erneuten Bereitstellung im Inventar freigegeben. Wenn die außer Betrieb genommene Festplatte aufgrund eines Hardwarefehlers nicht gelöscht werden kann, wird sie sicher aufbewahrt, bis sie zerstört werden kann. Jede Einrichtung wird regelmäßig überprüft, um die Einhaltung der Richtlinie zum Löschen von Datenträgern sicherzustellen.

4. Sicherheitsanforderungen an die Beschäftigten.

Das Personal von Google muss sich in Übereinstimmung mit den Unternehmensrichtlinien in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Gepflogenheiten und professionelle Standards verhalten.

Google führt zumutbare und angemessene Hintergrundüberprüfungen im gesetzlich zulässigen Umfang und in Übereinstimmung mit den geltenden lokalen arbeitsrechtlichen und gesetzlichen Vorschriften durch.

Das Personal muss sich einer Vertraulichkeitsvereinbarung unterwerfen und den Erhalt und die Einhaltung der Vertraulichkeits- und Datenschutzrichtlinien von Google bestätigen. Das Personal erhält Sicherheitstrainings. Personal, das Kundendaten verarbeitet, muss zusätzliche Anforderungen erfüllen, die dieser Rolle entsprechen (z. B. Zertifizierungen). Das Personal von Google verarbeitet Kundendaten nicht ohne Genehmigung.

5. Sicherheitsanforderungen an Subunternehmer.

Vor dem Einbinden eines Subunternehmens führt Google eine Prüfung der Sicherheits- und Datenschutzpraktiken des Subunternehmens durch, um sicherzustellen, dass das Subunternehmen ein Maß an Sicherheit und Datenschutz bietet, das dem Zugriff auf Daten und dem Umfang der von diesem erbrachten Dienste entspricht. Nachdem Google die bei einem Subunternehmen gegebenen Risiken bewertet hat, muss das Subunternehmen in Vertragsklauseln betreffend Sicherheit, Vertraulichkeit und Datenschutz einwilligen.

6. Datenschutzbeauftragter.

Der Datenschutzbeauftragte von Google kann kontaktiert werden unter: enterprise-dpo@google.com

Stand: 18.12.2019