Vereinbarung zur Auftragsverarbeitung zwischen

Siehe Angaben zum Kunden
– nachfolgend Auftraggeber genannt –

und

STOTaX GmbH & Co. KG
Dechenstrasse 7
53115 Bonn
– nachfolgend Auftragnehmer genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer führt die im Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien werden dort beschrieben. Sofern der Auftragnehmer Zugriff auf Daten hat, die dem Berufsgeheimnis des Auftraggebers im Sinne von § 203 StGB unterliegen, gelten ergänzend die speziellen Regelungen des Anhangs 4.

(2) Diese Vereinbarung gilt, sofern keine anderweitigen Regelungen vereinbart wurden, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

§ 2 Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend vom Auftraggeber zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragnehmer dies verlangt.

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Maßnahmen zu treffen und im Anhang 3 dieser Vereinbarung zu dokumentieren. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragnehmer darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragnehmer dem Auftraggeber nur wesentliche Anpassungen mitteilen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragnehmer bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit, insbesondere bezüglich solcher Geheimnisse dem Auftraggeber im Sinne von § 203 StGB, verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragnehmer darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seinen bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Dadurch entstehende Aufwände werden vom Auftraggeber übernommen. Auskünfte an die betroffene Person oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(8) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Artikeln 32 bis 36 DS-GVO genannten Pflichten. Der Auftragnehmer wirkt u.a. bei der Erstellung einer Datenschutz-Folgenabschätzung und ggfs. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Er hat dem Auftraggeber alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen. Die Aufwände, die im Rahmen der in diesem Absatz genannten Unterstützungshandlungen entstehen, werden vom Auftraggeber übernommen.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsnehmer ist berechtigt weitere Auftragsnehmer zu beauftragen. Er informiert den Auftraggeber über die eingesetzten weiteren Unterauftragnehmer sowie über geplante Änderungen durch Hinzuziehung oder Ersetzung. Sofern Einwände bestehen, hat der Auftraggeber einen etwaigen Einspruch unverzüglich zu erheben.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragnehmer weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich diese Vereinbarung bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn der Auftragnehmer durch eine schriftliche Vereinbarung sicherstellt, dass die in dieser Vereinbarung vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der getroffenen Vereinbarung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieser Vereinbarung genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der getroffenen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs und nach rechtzeitiger vorheriger Anmeldung. In diesem Zusammenhang entstehende Aufwände werden vom Auftraggeber übernommen.

Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragnehmers zur Dokumentation der Maßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße des Auftragnehmers

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Maßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggfs. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Auftraggeber unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieser Vereinbarung oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(2) Änderungen dieser Vereinbarung und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anhang 1: Auflistung der beauftragten Dienstleistungen

Gegenstand der Verarbeitung	**Stotax Kanzlei** Überlassung und Installation von spezieller Branchensoftware (Steuerwesen, Rechnungswesen, Jahresabschluss inklusive Anlagenverwaltung, Lohnabrechnung, optional: SBS Lohn, ggfs. auch für Mandaten, Kanzleimanagement inklusive DMS-System), womit der Auftraggeber Steuererklärungen, Steuerberechnungen, die Finanzbuchhaltung und Lohnabrechnungen erstellen bzw. die Buchführung durchführen kann. **Stotax Betrieb** Überlassung und Installation von spezieller Branchensoftware (Steuerwesen, Rechnungswesen, Jahresabschluss inklusive Anlagenverwaltung, Lohnabrechnung), womit der Auftraggeber Steuererklärungen, Steuerberechnungen, die Finanzbuchhaltung und Lohnabrechnungen erstellen bzw. die Buchführung durchführen kann. Die *Softwarelinie KMU* ist die Lösung für Abteilungen in gewerblichen Unternehmen, die sich auf die Bereiche Rechnungswesen und Lohnabrechnung spezialisiert haben. Die *Softwarelinie Konzern* ist die Lösung für Steuerabteilungen im Konzern, die sich auf die Bereiche Jahresabschluss und Erstellung von Steuererklärungen spezialisiert haben. **Stotax Kontor** Überlassung und Installation von spezieller Branchensoftware (Steuerwesen, Rechnungswesen, Jahresabschluss inklusive Anlagenverwaltung, Lohnabrechnung, optional: SBS Lohn, ggfs. auch für Mandaten), womit der Auftraggeber die Finanzbuchhaltung, den Jahresabschluss inkl. Anlagenverwaltung und Lohnabrechnungen erstellen bzw. die Buchführung durchführen kann. **Stotax Gehalt und Lohn** Überlassung und Installation von spezieller Branchensoftware. Durch die Software wird der Auftraggeber mit einem einfachen Workflow, einem vollintegrierten Arbeitnehmer-Meldemanager, der Vorbelegung aller wichtigen Lohnarten u.a. Urlaubsgeld, Weihnachtsgeld, SFN-Zuschläge, VWL, Direktversicherungen, übersichtlichen Auswertungen und Statistiken sowie einem umfassenden Hilfesystem mit Leitfäden bei der Durchführung der Finanzbuchhaltung, bei der Erstellung von Lohnabrechnungen und bei der Buchführung unterstützt. **Stotax Select** Bereitstellung von Cloud-Anwendungen auf der Online-Digitalplattform Stotax Select. Diese Plattform unterstützt die digitale und papierlose Zusammenarbeit zwischen Berater und Mandant. **IT-Support und Online-Nutzung**

	IT-Support (Installation, Analyse von Fehlersituationen und Fernwartung) in Bezug auf die dem Auftraggeber überlassene Software. Betrieb und Pflege von Stotax Select und der Online-Nutzung der Branchensoftware (inkl. Datensicherung, Wartung und Aktualisierung der Systeme). **Leistungsbeschreibungen** Zudem ergibt sich Gegenstand sowie Art und Zweck der Verarbeitung aus dem jeweiligen Hauptvertrag und den dazugehörigen Leistungsbeschreibungen. Die detaillierten Leistungsbeschreibungen zu den o.g. Produkten stehen auf der Homepage von Stotax unter dem folgenden Link zur Verfügung. https://www.stollfuss.de/service/media-center.aspx
Art und Zweck der Verarbeitung	Art der Verarbeitung: Der Auftragnehmer unterstützt den Auftraggeber durch die Bereitstellung der Branchensoftware sowie zusätzlich bei Stotax Select und einer Online Nutzung der Branchensoftware durch die Bereitstellung der Infrastruktur, bei der Erstellung von Steuererklärungen, von Steuerberechnungen, von Finanzbuchhaltung und von Lohnabrechnungen. Der Auftragnehmer ist bei der Online Nutzung (Stotax Select und Branchensoftware) mit der Verarbeitung und Speicherung von Daten beauftragt. Zweck der Verarbeitung: Zweck der Datenverarbeitung ist die Erstellung bzw. Unterstützung bei der Erstellung von Steuererklärungen, Steuerberechnungen, Jahresabschlüssen, Finanzbuchhaltungen und Lohnabrechnungen. Die genannten Erklärungen/Abrechnungen erstellen die Auftraggeber entweder für ihre Mandanten/Kunden oder für sich selbst.
Art der personenbezogenen Daten	Die Software ermöglicht die Verarbeitung folgender Arten personenbezogener Daten: 1. Daten der Mandanten / Kunden des Auftraggebers: Name, Adresse, Geburtsdatum, Geburtsort, Geschlecht, Familienstand, Staatsangehörigkeit, Telefon, E-Mail, Steuernummer, Steuer-IdNr., Steuerdaten, Finanzamt, Beruf, Gehalt, Einkünfte, Fehlzeiten, Art der Fehlzeiten, Bankverbindungen, Sozialversicherungsnummer, Krankenversicherung, Rentenversicherung 2. Ggfs. Mitarbeiterdaten der Mandanten / Kunden des Auftraggebers: s.o. 3. Ggfs. Mitarbeiterdaten des Auftraggebers: s.o. 4. Besondere Kategorie personenbezogener Daten: Konfession, Gewerkschafts-, Parteizugehörigkeit, krankheitsbedingte Fehlzeiten von Mandanten / Kunden des Auftraggebers

Kategorien betroffener Personen	1. Mitarbeiter und Kunden / Mandanten des Auftraggebers 2. Mitarbeiter, Familienangehörige und Kunden von Kunden / Mandanten des Auftraggebers 3. Ggfs. andere Personen, auch als Verbraucher, sofern sie Nutzer einer Leistung des Auftraggebers sind

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
CANCOM Managed Services GmbH Erika-Mann-Straße 69 80636München	Köln / Hamburg (RZ)	Bereitstellung und Wartung der IT Infrastruktur im Rechenzentrum für Stotax Select und Branchensoftware (asp.net)
DATAGROUP Köln GmbH Schanzenstraße 6 – 20 51063 Köln	Köln / Frankfurt a.M. (RZ)	Bereitstellung und Wartung der IT Infrastruktur im Rechenzentrum für Stotax Select und Branchensoftware (asp.com) IT-Support für die Stotax Online Nutzung und die lokalen Stotax Installationen beim Kunden vor Ort
Wolters Kluwer Software und Service GmbH SBS Zentrale Pforzheimer Straße 46/1 75015 Bretten	Rechenzentren in Deutschland	Bereitstellung ADDISON Datenservice in Verbindung mit SBS Lohn
Goldstein Softwaresysteme e.K. Ostseestraße 107 10409 Berlin	Berlin	Support für die Stotax Online (SBS Lohn) Nutzung und die lokalen Stotax Installationen (SBS Lohn) beim Kunden vor Ort

Anlage 3: Technisch-organisatorische Maßnahmen

1. Technisch-organisatorische Maßnahmen, Art. 32 DS-GVO

Zum Schutz von personenbezogenen Daten, die Stotax GmbH & Co. KG (nachfolgend Stotax) von ihren Kunden zum Zwecke der Auftragsdatenverarbeitung i. S. v. Art. 28 DS-GVO erhalten hat, hat Stotax technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO getroffen.

2. Zutrittskontrollmaßnahmen zu Serverräumen

Die eigenen Serverräume befinden sich im Hauptgebäude des Unternehmens sowie in einem in unmittelbarerer Nähe gelegenen unabhängigen Nebengebäude und sind mittels einer Einbruchmeldeanlage alarmgesichert. Im Falle eines Alarms wird der beauftragte Wachdienst über den Alarm informiert. Der Serverraum im Hauptgebäude ist fensterlos und mit einem elektronischen Schließsystem (RFID) versehen. Die Zutrittsrechte werden personifiziert vergeben. Es werden sowohl erfolgreiche als auch erfolglose Zutrittsversuche protokolliert. Die Fenster des Serverraums im Nebengebäude sind vergittert, alarmgesichert und abschließbar. Der Serverraum ist mit einem mechanischen Schloss versehen. Es werden regelmäßige Kontrollgänge von einem beauftragten Wachdienst durchgeführt.

3. Zutrittskontrollmaßnahmen zu Büroräumen

Das Gebäude ist mit einem elektronischen Schließsystem (RFID) versehen und mittels einer Einbruchmeldeanlage gesichert. Wenn die Einbruchmeldeanlage ausgelöst wird, wird der beauftragte Wachdienst informiert. Die Zutrittsrechte werden personalisiert vergeben und die Zutrittsversuche protokoliert. Zudem werden die Zugänge zu dem Bürogebäude videoüberwacht. Daneben existieren mechanische Schlösser für das Gebäude und die Büroräume. Die Schlüsselausgabe wird protokolliert. Für betriebsfremde Personen sind Zutrittsregeln festgelegt. Es werden regelmäßige Kontrollgänge von einem beauftragten Wachdienst durchgeführt.

4. Zugangs- und Zugriffskontrollmaßnahmen

Ein differenzierendes Berechtigungskonzept regelt den Zugriff der Mitarbeiter auf die Daten. Es existiert ein definierter Freigabeprozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen. Die Mitarbeiter haben sich über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst zu authentisieren. Im Unternehmen existieren verbindliche Passwortparameter. Die Nutzer werden durch das IT-System zur Einhaltung der Passwortvorgaben gezwungen. Der Bildschirm wird bei Inaktivität des Benutzers gesperrt. Bei Verlust, Vergessen oder Ausspähen eines Passworts vergibt der Administrator ein neues Initialpasswort. Die Anzahl erfolgloser Anmeldeversuche ist auf drei Versuche begrenzt. Wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde, bleiben die Zugänge für einen festgelegten Zeitraum gesperrt. Die Authentisierung bei Fernzugängen erfolgt über ein VPN-Zertifikat und ein Passwort. Die Anzahl von erfolglosen Anmeldeversuchen bei Fernzugängen ist auf 3 Versuche beschränkt. Die Zugänge bleiben für einen festgelegten Zeitraum gesperrt, wenn die maximale Anzahl erfolgloser Anmeldeversuche erreicht worden ist. Die Systeme, auf denen personenbezogene Daten verarbeitet werden, sind über eine Firewall abgesichert, die regelmäßig aktualisiert wird. Die Firewall wird von der eigenen IT administriert.

5. Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten

Nicht mehr benötigte Papier-Unterlagen (bspw. Ausdrucke / Akten / Schriftwechsel) werden über Schredder oder über verschlossene Datentonnen, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden, entsorgt. Nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, werden von der eigenen IT physikalisch zerstört. Mobile Datenträger dürfen im Unternehmen nur von einem restriktiv eingeschränkten Personenkreis verwendet werden. Ansonsten ist eine technische Sperrung

eingerichtet. Die Mitarbeiter dürfen keine privaten Datenträger verwenden. Alle benötigten Speichermedien werden vom Unternehmen gestellt. Auf eigenen privaten Geräten werden keine personenbezogenen Daten verarbeitet. Daten auf mobilen Endgeräten (Notebooks) werden verschlüsselt.

6. Maßnahmen zur sicheren Datenübertragung

Die verschlüsselte Transferierung personenbezogener Daten erfolgt per verschlüsselter Datei als Mailanhang, per VPN, per https/TLS oder per SFTP. Die Verwaltung der Schlüssel bzw. der Zertifikate erfolgt über die eigene IT. Übertragungsvorgänge werden protokolliert.

7. Maßnahmen zur Sicherstellung der Verfügbarkeit

7.1 Serverraum

Die Serverräume verfügen über eine feuerfeste bzw. feuerhemmende Zugangstür und sind mit einem Löschsystem (CO2 Löscher) ausgestattet. Die Außenwände bestehen aus einer Massivwand. Die Serverräume sind klimatisiert und verfügen über eine unterbrechungsfreie Stromversorgung. Der Serverraum im Nebengebäude ist mit Rauchmeldern ausgestattet und an eine Brandmeldezentrale angeschlossen. Die genannten Funktionalitäten werden regelmäßig getestet.

7.2 Backup- und Notfall-Konzept, Virenschutz

Es existiert ein Backupkonzept, dessen Funktionalität der Backup-Wiederherstellung regelmäßig getestet wird. Backups von Systemen, auf denen personenbezogene Daten gespeichert sind, werden täglich und als Echtzeitspiegelung angefertigt. Die Backups werden auf einem zweiten redundanten Server und auf Sicherungsbändern gespeichert. Der Aufbewahrungsort der Backups befindet sich in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil. Im Falle eines Transports der Backups werden diese von Mitarbeitern der eigenen IT mitgeführt. Es existiert ein dokumentierter Prozess zum Software – bzw. Patchmanagement, wofür die eigene IT verantwortlich ist. Es existiert ein Notfallkonzept. Die IT-Systeme sind technisch vor Datenverlust / unbefugten Datenzugriffen mittels stets aktualisiertem Virenschutz und Spamfilter geschützt.

7.3 Netzanbindung

Das Unternehmen verfügt über eine redundante Internetverbindung, wofür die eigene IT verantwortlich ist.

8. Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen

Regelmäßige interne Bewertung und Prüfung der eingesetzten Technologie und Maßnahmen. Beratung und Prüfung durch Hersteller und verschiedenen externe Partnerfirmen.

Anhang 4: Ergänzende Vereinbarung zur Wahrung des Berufsgeheimnisses

Da aufgrund der Dienstleistung nicht ausgeschlossen werden kann, dass der Auftragnehmer Informationen des Auftraggebers zur Kenntnis nimmt, die einer beruflichen Schweigepflicht unterliegen, bzw. den Auftragnehmer als Dienstleister an der beruflichen Tätigkeit des Auftraggebers, die einer beruflichen Verschwiegenheitsverpflichtung unterliegt, mitwirkt, gilt die nachfolgende Vereinbarung in Ergänzung der Vereinbarung zur Auftragsverarbeitung.

§ 1 Schweigepflicht des Berufsgeheimnisträgers

Durch die Kenntnisnahme der dem Berufsgeheimnis unterliegenden Daten durch den Auftragnehmer liegt ein Offenbaren im Sinne des § 203 StGB vor.

Diese Offenbarung ist strafrechtlich nicht relevant, soweit dies für die Inanspruchnahme der Tätigkeit des Auftragnehmers erforderlich ist. Gleiches gilt für Offenbarungen seitens des Auftragnehmers gegenüber deren Auftragnehmer (Unterauftragnehmer des Auftraggebers), die etwa in mehrstufigen Unterauftragsverhältnissen eingeschaltet werden. Gegenüber einem IT-Dienstleister ist das Offenbaren erforderlich, damit der Berufsgeheimnisträger dessen Tätigkeit (Wartung, Einrichtung etc. der IT-Anlagen) in Anspruch nehmen kann.

§ 2 Verpflichtung zur Geheimhaltung

Der Auftragnehmer wird verpflichtet,

- eine Kenntnisnahme der Daten, die dem Berufsgeheimnis unterliegen, auf das Erforderliche zu beschränken,
- die Verarbeitung der Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Pflichten durchzuführen,
- für die Verarbeitung nur die Mitarbeiter einzusetzen, die durch den Auftragnehmer schriftlich auf die Verschwiegenheit nach § 203 StGB verpflichtet wurden.
- für die Verarbeitung nur die Subunternehmer einzusetzen, die durch den Auftragnehmer auf die Verschwiegenheit nach § 203 StGB verpflichtet wurden. Ferner müssen die Subunternehmer die gleichen Anforderungen erfüllen, die der Auftragnehmer aus dieser Vereinbarung trifft.

§ 3 Zeugnisverweigerungsrecht

Dem Auftragnehmer ist bekannt, dass hinsichtlich der dem Berufsgeheimnis unterliegenden Daten ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweigerung entscheidet der Berufsgeheimnisträger des Auftraggebers.

§ 4 Beschlagnahmeverbot

Dem Auftragnehmer ist bekannt, dass die dem Berufsgeheimnis unterliegenden Daten, die sich im Gewahrsam des Auftragnehmers zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 2 S. 2 StPO unterliegen. Einer Sicherstellung ist zu widersprechen.

Der Auftraggeber ist unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht.