Vereinbarung zur Auftragsverarbeitung gemäß Art.28 DS-GVO

zwischen

Mobildiscothek flamenco de luxe
Hermann - von - Helmholtz - Straße 6, 04626 Schmölln, Deutschland
(im Folgenden Auftraggeber oder Kunde genannt)

und

Odacer Finanzsoftware GmbH
Konrad-Adenauer-Ring 13, 65187 Wiesbaden
(im Folgendenden Auftragnehmer genannt)

Präambel

Der Auftraggeber nutzt die Cloud-Plattform "Papierkram.de" des Auftragnehmers zur Verwaltung seiner betrieblichen Buchhaltung. Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 Datenschutz-Grundverordnung (im Folgenden: DS-GVO) als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Auftragsdatenverarbeitung ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt.

Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 DS-GVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung. Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der bestehenden Vertragsbeziehung (in Folgenden: Leistungsvereinbarung) und der dort in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben.

Grundsätzlich ist der Auftraggeber für die Einhaltung der Vorschriften der DS-GVO und anderer Vorschriften über den Datenschutz verantwortlich und behält insofern die Herrschaft über die zu verarbeitenden Daten. Der Auftragnehmer wird den Auftraggeber hierbei in geeigneter Weise unterstützen.

1. Begriffsbestimmungen

Sofern in diesem Vertrag der Begriff "Datenverarbeitung" oder "Verarbeitung" (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten i.S.d. Art. 4 Nr. 2 DS-GVO verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer bietet mit Papierkram.de eine Cloud-Plattform für die Buchhaltung von Selbständigen und kleinen Unternehmen an. Die genauen Dienstleistungen des Auftrags ergeben sich aus dem oben genannten Vertrag.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

3. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

a. Zugriff auf die Software mittels administrativen Zugängen (Einrichtung, Schulung und Hilfe)
b. Überwachung der Parameter der eingesetzten zentralen Systemdienste (Monitoring)
c. Auswertung des proaktiven Monitorings zur technischen Problemerkennung (Betrieb)
d. Aktualisierung der Software durch planmäßige Updates und Patches (Fernwartung)
e. Außerplanmäßige Anpassungen, wenn erforderlich (Hotfixes)
f. Bearbeitung von Störungsmeldungen nach vereinbarten SLAs (Support)
g. Interne Dokumentation (Betriebshandbuch, Protokollierung der Maßnahmen, Schulungen)

Die Verarbeitung findet in Form des Zugriffs und der Veränderung von Daten auf dem System statt. Die Zweckerfüllung besteht in Installation, Unterstützung bei Betrieb und der Störungsbeseitigung des Systems.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers. Eine Verlagerung darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Die geeignete Garantie wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind jegliche durch den Auftraggeber in dem Dienst Papierkram.de gespeicherte Daten wie z.B.:

- Kundenstammdaten (Anschrift, Name)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Details zu getätigten Zahlungen

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Endkunden
- Beschäftigte
- Lieferanten
- Ansprechpartner

4. Technische und organisatorische Maßnahmen

(1) Die zum Zeitpunkt des Vertragsschlusses bestehenden technisch-organisatorischen Maßnahmen sind als Anhang 1 zu diesem Vertrag beigefügt. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 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 Anhang 1].

(3) Die technischen und organisatorischen Maßnahmen folgen dem Stand der Technik. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Ein Datenschutzbeauftragter ist gemäß Artt. 38 und 39 DS-GVO auf Grund der Unternehmensgröße nicht bestellt.
2. Pflichten des Auftragnehmers
    a. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer 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 Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
    b. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anhang 1].
    c. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
    d. Die unverzügliche Information des Auftraggebers 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 Auftragnehmer ermittelt.
    e. Soweit der Auftraggeber 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
    f. Der Auftragnehmer 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.
    g. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer 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 Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Firma Unterauftragnehmer	Anschrift / Land	Leistung
BLUEEND AG	Konrad-Adenauer-Ring 13 65187 Wiesbaden	Bereitstellung Server-Hardware und Infrastruktur im Rechenzentrum FFM und Falkenstein
Wildbit Inc.	225 Chestnut St. Philadelphia PA, 19106.	Bereitstellung Infrastruktur für den Versand und Empfang von E-Mails
NewRelic	88 Spear St., Suite 1200 San Francisco, CA USA 94105	Monitoring Infrastruktur und Dienste

b. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mit einer Frist von 14 Tagen vorab schriftlich oder in Textform anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer 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.

c. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Kunden mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Betriebsstätten zu überzeugen. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmers erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen;
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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
b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Weisungsbefugnis des Auftraggebers

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

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

11. Löschung und Rückgabe von personenbezogenen Daten

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

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

12. Haftungsregelungen

(1) Der Auftragsverarbeiter verantwortet insbesondere, aber auch nur:

a. Die weisungs- und zweckgemäße sowie mittelkonforme Verarbeitung der Daten,
b. inkl. Hinweispflicht bei rechtswidrigen Weisungen
c. Die Vertraulichkeitsverpflichtung der beteiligten befugten Personen,
d. Die ergriffenen technischen und organisatorischen Schutzmaßnahmen,
e. Die ordnungsgemäße Beauftragung von Unterauftragnehmern,
f. Die Mithilfe bei Wahrnehmung von Betroffenenrechten – soweit vereinbart,
g. Unterstützung bei Meldung von Datenschutzvorfällen,
h. Unterstützung bei Durchführung von Datenschutz-Folgeabschätzungen – soweit vereinbart,
i. Erstellung und Führung eines Verarbeitungsverzeichnisses der Verarbeitungstätigkeiten im Rahmen der Auftragsverarbeitungen,
j. Die Bestellung eines eigenen Datenschutzbeauftragten,
k. Ordnungs- und vertragsgemäße Löschung und / oder Rückgabe von Daten nach Abschluss der Verarbeitung sowie,
l. Duldung und Mitwirkung bei Prüfungen und Audits des für die Verarbeitung Verantwortlichen.

(2) Der Auftraggeber haftet für Verstöße gegen jeweils geltende europäische und deutsche Datenschutzbestimmungen.
Dies gilt insbesondere für:

a. Weisungen die gegen geltende europäische und deutsche Datenschutzbestimmungen verstoßen,
b. verspätete oder unterlassene Mitteilung der Geltendmachung von Rechten durch Betroffene oder ihre Vertreter,
c. verspätete oder unterlassene Mitteilung von Datenschutz- und/oder Informationssicherheitsvorfällen.

(3) Der Auftraggeber haftet für alle finanziellen Folgen wie:

a. Schadenersatzforderungen von Betroffenen,
b. Kosten des Auftragnehmers für die Minderung der Schäden des Datenschutzverstoßes,
c. zivilrechtliche Folgekosten von Verstößen gegen geltende europäische und deutsche Datenschutzbestimmungen.

03.06.2018 17:53:14 von Mobildiscothek flamenco de luxe digital akzeptiert

Anlagenverzeichnis

Anlage 1: Technisch- organisatorische Maßnahmen der odacer Finanzsoftware GmbH

Anhang 1: Technisch- organisatorische Maßnahmen der odacer Finanzsoftware GmbH

(1) Diese Anlage beschreibt die technisch- und organisatorischen Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO der odacer finanzsoftware GmbH (im Folgenden: papierkram.de) als Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d), um den Datenschutz gemäß DS-GVO zu gewährleisten.

(2) Papierkram.de bietet seinen Kunden als Auftragnehmer Dienstleistungen zur Erstellung und Verarbeitung von Dokumenten rund um das Thema Buchhaltung an. Diese werden auf Basis der Nutzungsbedingungen und Leistungsbeschreibungen erbracht (siehe: https://www.papierkram.de/agb/). Die primäre Datenverarbeitung von Kundendaten erfolgt auf der Multi-Domain-Plattform papierkram.de welche auf einem dedizierten Server-Cluster im Frankfurter Rechenzentrum betrieben wird. Die Webseite www.papierkram.de dient der öffentlichen Darstellung und wird im Falkensteiner Rechenzentrum betrieben. Der Betrieb aller Serversysteme wird durch die BLUEEND AG, Wiesbaden sichergestellt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Gewährleistung der Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

Pseudonymisierung
Sind in einem Verarbeitungsvorgang personenbezogene Daten nicht erforderlich, werden sie durch pseudonymisierende Identifikationsnummern ersetzt.

Verschlüsselung

- Kommunikation zwischen den Endgeräten der Kunden und den Servern der Plattform papierkram.de ("Data In Transit") wird per SSL/TLS verschlüsselt.
- Nutzdaten auf den Servern der Plattform papierkram.de ("Data In Use") werden in der Regel nicht verschlüsselt.
- Daten die nicht zum Betrieb der Plattform papierkram.de notwendig sind ("Data In Rest") werden per Verschlüsselung der Volumes verschlüsselt (siehe auch: "Gewährleistung der Verfügbarkeit" hinsichtlich der Verschlüsselung der Backups).

Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Vertraulichkeit (Zutrittskontrolle)

Verwaltung
Konrad-Adenauer-Ring 13, 65187 Wiesbaden:

Die Büroräume der Odacer Finanzsoftware GmbH befinden sich in einem Bürokomplex. Das Gebäude wird durch einen Schließdienst betreut und ist für Unbefugte außerhalb von Werkzeiten nicht betretbar (Schließsystem an allen Eingängen, Tiefgarage und Durchgängen).
Die Büroräume der Odacer Finanzsoftware GmbH selbst werden durch ein elektronisches System abgesichert. Kritische Räume, wie Buchhaltung, Personalwesen und Technik sind zusätzlich abgesichert und nur autorisierten Mitarbeitern zugänglich.

Rechenzentren

Haupt-RZ
BLUEEND AG; Konrad-Adenauer-Ring 13, 65187 Wiesbaden
Betrieben durch: rh-tec Business GmbH / rh-tec AG; Frankenallee 71, 60327 Frankfurt am Main

Backup-RZ
BLUEEND AG; Konrad-Adenauer-Ring 13, 65187 Wiesbaden
Betrieben durch: Hetzner Online GmbH; Industriestrasse 25, 91710 Gunzenhausen

Die Server der Odacer Finanzsoftware GmbH sind im Rechenzentrum Frankfurt untergebracht, die Remote-Backup-Systeme in Falkenstein. Die Zugangssysteme sind in allen Rechenzentren mehrstufig und eine Kombination aus PIN Eingabe, Chip-Kontrolle sowie biometrischer Authentifizierung.

Vertraulichkeit (Zugangs, Zugriffs und Weitergabekontrolle)

Alle DV Systeme der Odacer Finanzsoftware GmbH sind mit Zugangskontrollen und Rechtemodellen versehen, die den Zugriff auf personenbezogene Daten sichern, einschränken und protokollieren. Im Zusammenhang mit Kundendaten werden folg. Systeme und Kontrollen eingesetzt, alle genannten System befinden sich in direktem Zugriff der Odacer Finanzsoftware GmbH (on premise RZ oder Büroräume – siehe oben):

- Alle Workstations erfordern eine Authentifizierung gegen ein ID Management (Active-Directory). Bei mobilen Geräten findet eine Verschlüsselung der Datenträger statt.
- Auf den Workstations werden keine Kundendaten dauerhaft gespeichert, die Ablage von Kundeinformation ist auf das abgesicherte Intranetsystem (Protokolliertes CRM und Versioniertes DMS) und das Mailsystem (inkl. Archivierung und Protokollierung) beschränkt.
- Serverzugriffe werden IP und mit passwortgeschützten Individual Zertifikaten abgesichert.
- Zugangsdaten die nicht individualisiert werden können (z.B. Zugang zum Internetdienstleister) liegen in einem verschlüsselten Password Management System. Zugriffe werden protokolliert und verschlüsselt.
- Das Netzwerk der Odacer Finanzsoftware GmbH wird durch eine aktuelle Firewall abgesichert. Mitarbeiter mit einer Berechtigung zur Heimarbeit wählen sich über eine verschlüsselte VPN Verbindung ein.
- Der mobile Zugriff auf Daten der Odacer Finanzsoftware GmbH erfordert die Nutzung von 2-Faktor Authentifizierung – in der Regel biometrisch.

Integrität (Eingabekontrolle)

- Die Verarbeitung von Kundendaten (Vertrags und Zahlungsdaten) findet auf der Plattform *.papierkram.de statt. Anfragen und Kommunikation mit dem Kunden erfolgen über das Ticketing-System. Wichtige Änderungen und Ereignisse in diesen Systemen werden unveränderlich protokolliert und für mindestens 3 Jahre gespeichert.
- Eingaben im geschützten Bereich des Kunden, werden soweit protokolliert, wie es zur Sicherung und Konformität der Grundsätze ordnungsgemäßer Buchführung (GoB) relevant sind.
- Werden zusätzlich oder abweichend zu den Nutzungsbedingen Tätigkeiten im Auftrag des Kunden gewünscht (z.B. im Rahmen der Support-Hilfe), wird diese Tätigkeit im Ticketing-System dokumentiert.

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

Beachtung des Trennungsgebots
Die Odacer Finanzsoftware GmbH betreibt Entwicklungs-, Test- und Produktivsysteme i.d.R. auf unterschiedlicher Hardware oder Virtualisierung um die Trennung von personenbezogenen Daten des Kunden zu gewährleisten.

Systeme auf denen mehrere Kunden Zugriff haben, wird die Trennung im technisch sinnvollen Rahmen im Verhältnis zur gespeicherten Information durchgeführt:

1. Jeder Kunde hat eine eigene Datenbank.
2. Jeder Kunde erhält einen getrennten Speicherbereich.
3. Jeder Kunde hat eine eigene (Sub-) Domain.
4. Physikalische Medien und Daten (Muster, Vorlagen, Medien und CDs) werden entweder in abgeschlossenen Containern (Kundenakten) gelagert, dem Kunden direkt zurückgesendet oder nach Bearbeitung vernichtet.

Gewährleistung der Verfügbarkeit
Maßnahmen zur Absicherung der Serversysteme gegen zufällige Zerstörung oder Verlust:

- Haupt-RZ Frankfurt: Drei Brandabschnitte, redundante USV und Dieselaggregate, Rauchfrüherkennung VESDA, CO^2 Brandbekämpfungsanlage.
- Backup-RZ Falkenstein: Redundante USV und Dieselaggregate, Türverriegelungssystem, Löschgasanlage, Rauchmelder, Feuchtigkeitssensoren und Luftdruckmesser.
- Alle Festplattenkonfigurationen als RAID1 / RAID10 (in Ausnahmefällen RAID5)

Die Odacer Finanzsoftware GmbH sichert die DV Systeme mit Hilfe eines CDP Systems:

- Backupzyklus liegt in der Regel bei 24h
- Backups werden auf dem Quellsystem verschlüsselt.
- Backups werden auf einem Drittsystem gelagert.
- Das Drittsystem liegt in einem separaten Brandabschnitt und wird regelmäßig zu einer Remote-Location (Backup-RZ Falkenstein) gespiegelt.
- Die Übertragung erfolgt inkrementell und verschlüsselt via SSL

Gewährleistung der Belastbarkeit der Systeme
In regelmäßigen Abständen werden Last- und Penetrationstests der Systeme durchgeführt.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Die verwendeten Systeme zur Sicherung (siehe Verfügbarkeitskontrolle) sind auf eine rasche Wiederherstellung ausgelegt. Die notwendigen Schritte werden im Rahmen des ISMS dokumentiert und regelmäßig getestet.

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

Datenschutz-Management
Die Odacer Finanzsoftware GmbH betrachtet Datenschutz-Management als wichtigen Teil der Informationssicherheit und richtet sich nach den Leitlinien der ISO27000 zur Informationssicherheit, um Prozesse und Maßnahmen zu dokumentieren, implementieren und regelmäßig zu überprüfen.

Incident-Response-Management
Beim Auftreten eines Incidents im Umgang mit personenbezogenen Daten setzt die Odacer Finanzsoftware GmbH auf eine klare und regelmäßig kommunizierte Datenschutzleitlinie, einem Notfallhandbuch und einem entsprechend dokumentierten Prozess im ISMS. Für die Kommunikation von Sicherheitsproblemen und kritischen Updates können Benachrichtigungen an alle Kunden geschickt werden.

Privacy by Design/Default (Art. 25 Abs. 2 DS-GVO)
Alle Prozesse und Systeme der Odacer Finanzsoftware GmbH sind zweckgerichtet und erfüllen eine datenschutzfreundliche Voreinstellung.

Auftragskontrolle
Die Auftragskontrolle wird über die Verträge mit Kunden, bzw. durch die Vereinbarung in der Auftragsdatenvereinbarung gewährleistet. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers.