Auftragsverarbeitungsvertrag

Zwischen dem **Nutzer** der mobilen App

- Auftraggeber -

und der

myStand technology GmbH
Bergweg 7,
04356 Leipzig

- Auftragnehmer -

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis (i.F. Hauptvertrag) über die Zurverfügungstellung der mobilen Anwendung (App) „myStand Leads“. Im Rahmen der Durchführung dieses Vertrages verarbeitet der Auftragnehmer personenbezogene Daten (als Auftragsverarbeiter) im Auftrag des Auftraggebers (als Verantwortlicher) gemäß den im Vertrag festgelegten Vorgaben ("Auftragsverarbeitung").

Bei der App handelt es sich um die Zurverfügungstellung einer technischen Infrastruktur, mittels derer der Auftraggeber insbesondere Visitenkarten, aber auch ähnliche Kontaktinformationen mit einem mobilen Endgerät auslesen und die auf der Visitenkarte enthaltenen Informationen in einem elektronischen Kontakt in der App speichern und exportieren kann.

Die App vereinfacht mithin das Übertragen von Visitenkarteninformationen in elektronische Formate. Bei diesen Kontakten handelt es sich ausschließlich um Kontakte des Auftraggebers selbst. Der Auftragnehmer stellt lediglich die technischen Möglichkeiten zur Digitalisierung der nicht einem Dateiformat vorhandenen Kontaktinformationen.

1. Vertragsparteien

Auftragnehmer ist die myStand technology GmbH, Bergweg 7, 04356 Leipzig. Auftraggeber ist der Nutzer, der sich gem. den Nutzungsbedingungen zur Nutzung der App registriert hat. Insbesondere auf Ziff. 1.1 und 7.4 der Nutzungsbedingungen wird verwiesen.

2. Gegenstand des Auftrages

2.1 Der Auftragnehmer führt im Auftrag des Auftraggebers für die Dauer der Vertragslaufzeit eine Verarbeitung personenbezogener Daten auf Grundlage des Hauptvertrages (Nutzungsbedingungen) aus. Es gelten für den folgenden Vertrag die Begriffsbestimmungen (Legaldefinitionen) der DSGVO und des BDSG.

2.2 Der sich aus dem Hauptvertrag ergebende Leistungsumfang durch Nutzung der App beinhaltet insbesondere – ohne dass hierdurch die Leistungspflichten neu definiert würden – folgende Verarbeitungsvorgänge:

- Nutzerprofilverwaltung (Profil in der App)
- Erzeugen einer Bilddatei von einer Visitenkarte oder ähnlichen Kontaktinformationen
- Auslesen der in der Bilddatei enthaltenen Texte (Kontaktinformationen)
- Erstellung eines elektronischen Kontaktes (digitalisierte Kontaktinformationen) in der App, der die ausgelesenen Kontaktinformationen beinhaltet
- Möglichkeit des Exports der Kontaktinformationen
- Möglichkeit, den Dritten über die Kontaktinformationen zu kontaktieren.

2.3 Bei dem Betrieb der App werden regelmäßig folgende Arten von personenbezogenen Daten verarbeitet:

- Benutzerinformationen, d.h. Daten des App-Anwenders selbst, in der Regel:
    - Name
    - Handynummer
    - Login-Daten
    - E-Mail-Adresse

- Personenbezogene Daten Dritter (Visitenkarteninhaber), dies regelmäßig in folgendem Umfang:
    - Name
    - Unternehmen / Arbeitgeber

- Telefonnummer / Mobilnummer
- Mailadresse
- Titel
- Positionsbezeichnung
- Unternehmensanschrift

2.4 Kreis der von der Datenverarbeitung Betroffenen:

- Kunden des Auftraggebers
- Dritte (Kontakte des Auftraggebers / Visitenkarteninhaber)
- Mitarbeiter des Auftraggebers

2.5 Dauer der Verarbeitung:

Die erhobenen personenbezogenen Daten werden für die Dauer der Vertragslaufzeit (Ziff. 3) verarbeitet oder solange eine gesetzliche Verpflichtung zur Verarbeitung (insbesondere zur Aufbewahrung) besteht.

3. Dauer und Beendigung des Auftrages

3.1 Die Wirkung dieser Vereinbarung tritt mit der erfolgreichen Registrierung des Nutzers zur Nutzung der mobilen App ein und gilt für die Dauer des Bestandes des Hauptvertrages.

3.2 Ein etwaiges außerordentliches Kündigungsrecht der Parteien bleibt hiervon unberührt; der Auftraggeber ist ohne Bestand des hiesigen Auftragsverarbeitungsvertrages oder eines entsprechenden Nachfolgevertrages nicht berechtigt, die App weiter zu nutzen und hat eine solche Nutzung in diesem Fall einzustellen.

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers / Kontrollbefugnisse

4.1 Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer sowie für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DS-GVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit für die Erfüllung der vorbezeichneten Pflichten des Auftraggebers erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DS-GVO nachkommen kann. Der Auftragnehmer ist verpflichtet, alle Anfragen Dritter, sofern sie erkennbar an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

4.2 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisungen). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst insbesondere Weisungen im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Der Auftraggeber ist aber nicht berechtigt, Weisungen im Hinblick auf Änderungen der Funktionalität der App zu erteilen.

4.3 Der Auftraggeber ist selbst und ausschließlich dafür verantwortlich, die datenschutzrechtliche Zulässigkeit der Digitalisierung analoger Kontaktinformationen Dritter (Visitenkarteninhaber) zu gewährleisten. Der Auftragnehmer ist nicht berechtigt und verpflichtet, eine Zulässigkeit der Speicherung der Daten Dritter (Betroffener) originär zu prüfen und ist nicht verpflichtet, die Betroffenen über die Datenspeicherung zu informieren (Art. 13, 14 DSGVO). Die Einhaltung dieser datenschutzrechtlichen Informationsverpflichtungen obliegt dem Auftraggeber. Der Auftraggeber ist als Verantwortlicher gem. Ziff. 4.1. insbesondere auch dafür verantwortlich, das Vorhandensein einer Rechtsgrundlage der Verarbeitung personenbezogener Daten Dritter und die daraus folgenden Informationspflichten (insb. Art. 13 DSGVO) zu gewährleisten.

4.4 Änderungen des Verarbeitungsgegenstandes (Ziff. 2) und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Eine Änderung der Funktionalitäten der App kann der Auftraggeber nicht verlangen.

4.5 Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei seiner Kontrolle feststellt.

4.6 Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

4.7 Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von

personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

4.8 Statt der Einsichtnahmen und der Vor-Ort-Kontrollen darf der Auftragnehmer den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse des Auftragnehmers oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

4.9 Die Ziff. 4.1 – 4.9 gelten sinngemäß für die Begehr des Auftraggebers, einen Subunternehmer des Auftragnehmers kontrollieren zu wollen. Diese Kontrollen sind unter Einbeziehung des Auftragnehmers durchzuführen, der von seinen eigenen entsprechenden Kontrollrechten Gebrauch macht. Der Auftraggeber ist berechtigt, zu Art und Umfang der Kontrolle Weisungen zu erteilen und eigenes Kontrollpersonal zu entsenden.

4.10 Für alle durch den Auftraggeber begehrte Kontrollen ist der Auftragnehmer berechtigt, von dem Auftraggeber ein Entgelt auf marktüblicher Basis nach billigem Ermessen zu verlangen. Maßgeblich für die Höhe des Entgeltes ist insbesondere der Umfang der durch die Kontrolle gebundenen Personalkapazitäten des Auftragnehmers sowie externe Verrechnungssätze der Mitarbeiter.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer führt ausschließlich die Tätigkeiten durch, die zur Erfüllung der beauftragten Leistungen erforderlich sind. Er führt sie ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Änderungen des Tätigkeitsfeldes und Verfahrensänderungen sind schriftlich zu vereinbaren. Der Auftragnehmer speichert oder verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf Weisung des Auftraggebers. Der Auftragnehmer hat die zur Durchführung des Hauptvertrages notwendigen Leistungen so auszuführen, dass er sich nur insoweit Kenntnis von fremden Geheimnissen verschafft, als dies zur Vertragserfüllung erforderlich ist.

5.2 Für sämtliche Mitarbeiter des Auftragnehmers gilt aufgrund ihrer Aufgabenstellungen die Vertraulichkeit nach Art. 28 Abs. 3 lit. b DS-GVO. Nach dieser Vorschrift ist es ihnen

untersagt, personenbezogene Daten unbefugt zu verarbeiten. Gem. Art. 28 Abs. 3 lit. b DS-GVO ist jeder Mitarbeiter verpflichtet, die Vertraulichkeit der verarbeiteten Daten zu wahren. Diese Verpflichtung besteht auch über das Ende seiner Tätigkeit im Unternehmen hinaus.

Der Auftragnehmer verpflichtet sich in diesem Kontext, nur solche Mitarbeiter zur Durchführung des Vertrages einzusetzen, die über Ihre Pflichten zur Vertraulichkeit und zur Einhaltung aller weiteren Datenschutzbestimmungen belehrt und auf die Rechtsfolgen von Verstößen (u.a. Strafbarkeit) hingewiesen wurden. Zudem setzt der Auftragnehmer davon unabhängig nur solche Mitarbeiter ein, bei denen keine Anhaltspunkte dafür ersichtlich sind, dass deren Verlässlichkeit eingeschränkt sein könnte. Darüber hinaus werden auch nur solche Mitarbeiter eingesetzt, die eine angemessene Ausbildung und/oder Berufserfahrung im Umgang mit personenbezogenen Daten Dritter und zur Durchführung der notwendigen Arbeiten des Hauptvertrages haben.

5.3 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten zum Zwecke der Durchführung des Hauptvertrages.

5.4 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten. Es gilt analog die Vergütungsregelung gem. Ziff. 4.10.

5.5 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

5.6 Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

5.7 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

5.8 Über datenschutzrelevante Vorfälle und Verstöße gegen die vertraglichen Regelungen unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.

5.9 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6. Unterauftragsverhältnisse mit Subunternehmen / Drittländer

6.1 Die vertraglich vereinbarten Leistungen aus dem Hauptvertrag erbringt der Auftragnehmer unter Einschaltung der in Anlage 2 genannten Subunternehmer. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern befugt. Der Auftragsnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Widerspricht der Auftraggeber den Änderungen und die Parteien erzielen keine einvernehmliche Lösung über das weitere Vorgehen, haben beide Parteien das Recht zur fristlosen Kündigung der Nutzungsvereinbarung Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist.

6.2 Ein Subunternehmerverhältnis im Sinne dieser Bestimmung liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistung anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen sowie Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung.

6.3 Die vertraglich vereinbarte Datenverarbeitung aus dem Hauptvertrag und aus allen Unterauftragsverhältnissen findet ausschließlich in einem solchen Land statt, dass

vollständig und unmittelbar den Regelungen der DSGVO unterliegt. Eine Verarbeitung in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

7. Haftung

7.1 Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

7.2 Der Auftragnehmer haftet gegenüber dem Auftraggeber nach den gesetzlichen Vorschriften, soweit im Folgenden nichts Abweichendes vereinbart ist.

7.3 Die Haftung des Auftragnehmers ist ausgeschlossen, soweit der Schaden auf einfacher Fahrlässigkeit beruht. Dies gilt nicht bei der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), d. h. Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglichen und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf, insbesondere solcher Pflichten, bei deren Verletzung die Erreichung des Vertragszwecks gefährdet ist. In diesem Fall ist die Haftung des Auftragnehmers auf den vertragstypischen und vorhersehbaren Schaden beschränkt. Die vorstehende Haftungsbeschränkung gilt nicht, wenn eine Verletzung des Lebens, des Körpers oder der Gesundheit eingetreten ist und/oder soweit der Auftragnehmer im Einzelfall eine Garantie übernommen hat.

8. Technische und organisatorische Maßnahmen

8.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO. Ein aktueller Stand dieser Maßnahmen ist dem Vertrag als Anlage 1 beigefügt.

8.2 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten und gesetzlich erforderlichen Standards nicht unterschreiten.

8.3 Die technischen und organisatorischen Maßnahmen kann der Auftragnehmer nach eigenem pflichtgemäßem Ermessen der technischen und organisatorischen Weiterentwicklung anpassen, sofern das allgemeine bisherige Schutzniveau erhalten bleibt.

9. Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine berechtigte Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen -also weder vorsätzlich noch grob fahrlässigen- Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

10. Datenschutzbeauftragte

10.1 Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Zum Zeitpunkt des Vertragsschlusses ist dies Frau Anke Bunsen als interne Datenschutzbeauftragte.

10.2 Die Parteien haben sich auf Anfordern der anderen Partei jederzeit den aktuellen Datenschutzbeauftragten mitzuteilen oder, sofern ein solcher nicht bestellt ist, den für den Bereich Datenschutz zuständigen Ansprechpartner.

11. Beendigung des Vorvertrages

11.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrages oder jederzeit auf dessen Anforderung alle ihm etwaig überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

11.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer binnen 4 Wochen nach erfolgter Löschungsanzeige zu kontrollieren

12. Schlussbestimmungen

12.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist. Sofern der Auftragnehmer dem Auftraggeber Datenträger überlässt, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten, sind diese Datenträger entsprechend durch den Auftraggeber als sein Eigentum zu kennzeichnen.

12.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

12.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

12.4 Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

12.5 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Leipzig.

_____	_____
Ort, Datum Auftraggeber	Ort, Datum Auftragnehmer

Anlage 1:
Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Der Auftragnehmer gewährleistet die folgenden technischen und organisatorischen Maßnahmen zur Gewährung eines angemessenen Schutzniveaus der Sicherheit personenbezogener Daten (Art. 32 DS-GVO):

1. Zutrittskontrolle

1.1 Gebäudezugang nur über Sicherheitsschließanlage

1.2 Abgetrennter Bereich des Rechenzentrums über eigenen Zugang mit Sicherheitsschließanlage

1.3 Alarmanlage mit Wachschutz auf Schaltung

1.4 redundante Klimaanlage

1.5 verschlossener Serverschrank

1.6 Sicherheitstüren (außerhalb der Geschäftszeiten stets verschlossen)

1.7 es existieren Maßnahmen zur Verhinderung und Meldung von Überfällen

1.8 Verteilerräume (Strom, Wasser, Gas, Telefon, Gefahrenmeldeanlage usw.) sind gegen unbefugten Zutritt gesichert

2. Zugangskontrolle

2.1 Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.

2.2 Die Komplexität von Passwörtern und Pins unterliegt Mindestanforderungen, die dem jeweiligen aktuellen Stand der Technik entsprechen

2.3 Etwaige Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.

2.4 Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit

aktuellen Updates und Patches versorgt werden, die dem jeweiligen Stand der Technik entsprechen.

2.5 Alle Mitarbeiter sind angewiesen und werden kontrolliert, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

2.6 Trennung von Produktiv-, Test-, und Administrations-Netzbereichen

2.7 Verschlüsselung von Datenträgern

3. Zugriffskontrolle

3.1 Ein Berechtigungskonzept regelt die Vergabe und den Entzug von Rechten

3.1 Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben.

3.2 Die Vernichtung von Datenträgern und Papier erfolgt im Einklang mit den datenschutzrechtlichen Bestimmungen.

3.4 Es existieren Arbeitsanweisungen und Kontrollen zum sicheren Umgang mit IT-Systemen

3.5 Beschränkter Zugriff auf Administration Umgebung

3.6 der Grundsatz des „aufgeräumten Schreibtischs“ und des „leeren Bildschirms“ wird aktiv umgesetzt

4. Trennungskontrolle

4.1 Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, verarbeitet er diese getrennt von Daten anderer Kunden.

5. Pseudonymisierung & Verschlüsselung

5.1 Ein administrativer Zugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit dieser nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

5.2 Dem Auftragnehmer ist ein Zugriff auf die in der App gespeicherten Kontakte des Auftraggebers nicht möglich.

6. Eingabekontrolle

6.1 Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

7. Weitergabekontrolle

7.1 Sicherung elektronischer Übertragungen wie folgt:

- VPN-Verbindungen
- verschlüsselte Ende zu Ende E-Mail
- Firewallsystemen
- Passwortübermittlung über sicheren zweiten Kanal
- Verschlüsselung bei Fernwartungsvorgängen

7.2 Sicherung bei einem etwaigen Transport

- verschlossener Behälter
- verschlüsselte Datenträger

8. Verfügbarkeit und Belastbarkeit

8.1 Brandschutzanlage

8.2 Überspannungsschutz und Notstromversorgungsanlage

8.3 unterbrechungsfreie Stromversorgung

8.4 Klimaanlage

8.5 Festplattenspiegelungen

8.6 tägliches Back-up

8.7 Diebstahlschutz durch Zugriffs-und Zugangskontrolle

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

9.1 Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt.

9.2 Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt.

9.3 Mitarbeiter sind geschult und auf die Vertraulichkeit verpflichtet, zudem werden diese regelmäßig in Bezug auf den Datenschutz sensibilisiert

9.4 Der Auftragnehmer hat ein effektives Meldesystem für die Meldung von Anfragen Betroffener und entdeckte Datenschutzpannen eingerichtet.

10. Auftragskontrolle

10.1 Mit Vertragspartnern werden erforderlichenfalls Verträge über Auftragsdatenverarbeitung geschlossen, die ein den hiesigen Maßnahmen entsprechendes Schutzniveau bieten.

10.2 Vertragspartner werden sorgfältig ausgewählt.

11. Datenschutzfreundliche Voreinstellung

11.1 Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Anlage 2 „Subunternehmer“

1. **Connectline GmbH, August-Bebel-Str. 68, 06108 Halle (Saale)**
2. **PingPool GmbH, Dittrichring 17, 04109 Leipzig**
3. **Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Irland**
4. **Amazon Web Services, Inc**