Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen	und
OPED GmbH Medizinpark 1 83626 Valley/Oberlaindern	das für die Nutzung der Software verantwortliche Unternehmen (Verantwortlicher)
im Folgenden: **Auftragnehmer**	im Folgenden: **Auftraggeber**

Inhaltsverzeichnis

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Bereitstellung einer Software zur Bilderkennung zur Dokumentation und Nachbehandlung.

2.2 Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 30 Tagen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2.3 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art:

> Erfassen, Organisation, Ordnen, Speicherung (z.B. Umordnung im Speicher), Auslesen, Abfragen, Verwendung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichten von Daten (z.B. von Duplikaten).

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

- Betrieb, Hosting, Wartung und Support der Software.

2.4 Kategorien der Betroffenen Personen und Art der Daten

Betroffene Personen	Datenarten
Anwender (Patienten)	Vor- und Zuname, Geburtsdatum, Größe, Gewicht, Geschlecht, Sportart, Indikation, Behandlungsbeginn, OP-Datum, Unfalldatum, Behandlungs-ID, Ergebniswerte der Messung, Schmerzlevel

3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Verschwiegenheitsverpflichtung, Hinweis auf § 203 StGB: Der Auftragnehmer ist zur Verschwiegenheit verpflichtet, auch nach Beendigung des Auftrags. Diese Pflicht bezieht sich auf alles, was dem Auftragnehmer im Rahmen seiner Tätigkeit für den Auftraggeber bekannt wird. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(6) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(7) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(8) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(9) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(10) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(11) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

(12) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art.27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

4 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Die Verarbeitung von Daten in Privatwohnungen erfolgt nicht.

(7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(8) Der Auftragnehmer gewährleistet ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d DS-GVO.

5 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6 Unterauftragsverhältnisse

(1) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung des Subunternehmers informiert der Auftragnehmer den Auftraggeber.
Der Auftraggeber hat das Recht innerhalb von zwei Wochen ab Kenntnis der Information über den Subdienstleister aus wichtigem Grund schriftlich beim Auftragnehmer Einspruch gegen den Einsatz des Subunternehmers einzulegen. Erfolgt kein Einspruch innerhalb der genannten Frist, gilt dies als Zustimmung des Auftraggebers zum Einsatz dieses Subdienstleisters.

(3) Subunternehmern sind vertraglich mindestens die Datenschutzverpflichtungen auferlegt, die in den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(4) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(5) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(6) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(7) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(8) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(9) Es werden nur Subunternehmen innerhalb der EU oder des EWR beauftragt

(10) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(11) Kommt der Subunternehmer seinen Datenschutzverpflichtungen nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort, zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 4 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 Datenschutz-Grundverordnung zu enthalten.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

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

11 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

12 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(4) Der Auftragnehmer ist zur außerordentlichen Kündigung berechtigt, sofern der Auftraggeber der Beauftragung eines Subunternehmers gem. Kapitel 6 (1) dieses Vertrages widerspricht und keine Einigung erreicht werden kann.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von sämtlichen Ansprüchen Dritter frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden.

(3) Der Auftragnehmer haftet dem Auftraggeber gegenüber nur bei grober Fahrlässigkeit oder Vorsatz.

14 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) 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.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 2.

1. Organisation der Informationssicherheit
2. Personalsicherheit
3. Verwaltung der Werte
4. Zugangssteuerung
5. Kryptographie
6. Physische und umgebungsbezogene Sicherheit
7. Betriebssicherheit
8. Kommunikationssicherheit
9. Anschaffung, Entwicklung und Instandhaltung von Systemen
10. Lieferantenbeziehungen
11. Handhabung von Informationssicherheitsvorfällen
12. Informationssicherheitsaspekte beim Business Continuity Management
13. Compliance

1 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Nachstehend wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt sind. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen. Die Struktur orientiert sich nach der international anerkannten Norm DIN ISO/IEC 27002.

1.1 Leitlinie

Die Datenschutzleitlinie der OPED GmbH beinhaltet die Leitaussagen der Geschäftsleitung zum Umgang mit personenbezogenen Daten im Unternehmen. Alle Beschäftigten, freie Mitarbeiter und unterstützende Unternehmen sind verpflichtet diese zentralen Regelungen zu beachten.

Das erreichte IT-Sicherheitsniveau der Organisationseinheiten, Prozesse und Systeme wird durch eine Kombination aus periodisch wiederkehrenden Prüfungen und kontinuierlichen Kontrollen überwacht.

Die Überwachungen des laufenden Betriebs erfolgen in Abstimmung mit dem Sicherheitsbeauftragten.

Ein Review der Sicherheitspolitik erfolgt zumindest jährlich, soweit nicht eine essentielle Änderung dies früher erfordert. Hierdurch wird die laufende Angemessenheit, Eignung und Effektivität der Regelung sichergestellt.

Der Sicherheitsbeauftragte ist der Verantwortliche für die Sicherheitspolitik und hat die Verantwortung, diese zu entwickeln, zu überarbeiten und zu prüfen.

1.2 Organisation der Informationssicherheit

Die Führungskräfte der OPED GmbH sind in ihrer Organisationseinheit für die vollständige Umsetzung der Grundsätze der IT-Sicherheit und für die Erfüllung der an sie gestellten IT-Sicherheitsaufgaben verantwortlich.

Informationssicherheitsrollen und -verantwortlichkeiten sind in der IT-Sicherheitsorganisation definiert. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte unseres Unternehmens zu reduzieren.

Wir verfügen über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutz- und Informationssicherheitsvorfälle rechtzeitig gemeldet werden.

Auch pflegen wir laufenden Kontakt zu speziellen Interessensgruppen, um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

In unseren Projekten ist Datenschutz und Datensicherheit Bestandteil aller Phasen unserer Projektmethodik.

Durch unsere jeweiligen Richtlinien und Prozesse zur Telearbeit und der Nutzung von Mobilgeräten, stellen wir den Datenschutz und die Datensicherheit auch in diesen Bereichen sicher.

1.3 Personalsicherheit

Wir haben unsere Mitarbeiter sorgsam ausgewählt und ihre Eignung für ihre Rolle im Unternehmen überprüft. Ihre Verantwortlichkeiten haben wir in Funktionsbeschreibungen festgelegt und gleichen regelmäßig ab, ob die Mitarbeiter diesen entsprechen. Vor Beginn ihrer Anstellung unterschreiben alle Mitarbeiter eine Vertraulichkeits- sowie Datenschutzvereinbarung, die über die Beendigung des Beschäftigungsverhältnisses hinaus gilt. Die Mitarbeiter werden im Bereich Datenschutz- und Datensicherheit geschult, insbesondere werden Schulungen bei Funktionswechsel noch einmal aufgefrischt. Sie sind sich daher ihrer Verantwortung diesbezüglich bewusst.

In einem dokumentierten Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses stellen wir sicher, dass personenbezogene Daten geschützt und die Datensicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

1.4 Verwaltung der Werte

Sämtliche Werte (wie z.B. Betriebsmittel, Wechseldatenträger, Notebooks) und Informationen, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und gepflegt.

Wir haben zum Schutz dieser Werte Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt. Die Rückgabe erfolgt dokumentiert.

Unsere Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet.

Diesem Klassifizierungsschema entsprechend, haben wir dokumentierte Verfahren für die Handhabung unserer Werte, insbesondere auch unserer Wechseldatenträger, entwickelt und umgesetzt. Wir verfügen über einen dokumentierten und geregelten Prozess zum Transport von Datenträgern, um diese vor unbefugtem Zugriff, Missbrauch oder Verfälschung zu schützen.

Nicht mehr benötigte Datenträger entsorgen wir sicher, unter Anwendung eines dokumentierten Verfahrens und verpflichteter zertifizierter Dienstleister.

1.5 Zugriffssteuerung

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten zu ermöglicht.

Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.

Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern.

Ist- und Soll-Zustand von Benutzerzugangsrechten werden regelmäßig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.

Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

1.6 Kryptographie

Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt. Zu diesem Zwecke haben wir Regelungen über den Einsatz von Kryptographischen Maßnahmen im Unternehmen implementiert, die auch die Verwaltung von kryptographischen Schlüsseln umfasst und dem Schutzbedarf angemessen ist.

1.7 Physische und umgebungsbezogene Sicherheit

Wir haben dokumentierte und geregelte Maßnahmen getroffen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Diese umfassen unter anderem:

- Die Geschäftsräume liegen im 1. Stock eines Bürogebäudes und werden exklusiv genutzt.
- Türen zu Sicherheitsbereichen sind stets geschlossen. Schutz erfolgt über ein Token basiertes System
- Besucher oder externe Dienstleister werden individuell eingelassen.
- Der Brandschutz wird beachtet
- Es sind Sicherheitsbereiche vorhanden, zu denen nur eigens hierzu Berechtigte Zutritt erhalten.
- IT-Räume sind separat verschlossen und nur durch Berechtigte zu öffnen.
- Versorgungseinrichtungen werden vor Stromausfällen und Störungen geschützt
- Die Sicherheit der Verkabelung wird beachtet
- Die Instandhaltung von Systemen wird geplant oder umgesetzt
- Das Entfernen und Änderungen von Systemen und Informationen erfolgt geregelt.
- Die Sicherheit von Systemen außerhalb der Räumlichkeiten wird beachtet.
- Die Entsorgung oder Wiederverwendung von Betriebsmitteln erfolgt geregelt

- Unbeaufsichtigte Benutzergeräte werden durch Verschlüsselung geschützt
- Richtlinien für Clean Desk und Bildschirmsperren werden umgesetzt.

1.8 Betriebssicherheit

Wir verfügen über geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen u.a. die Steuerung im Falle einer Änderung an den informationsverarbeitenden Einrichtungen, als auch eine Steuerung und regelmäßige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen. So werden z.B. unter anderen folgende Werte laufend aktuell überwacht:

- Festplattenstatus und verfügbarer Speicher
- Raid-Status
- Dienste und Status aller virtuellen Maschinen
- Fehlerhafte Anmeldeversuche
- Speicherbelegung der Storages und Hauptspeicher
- Auslastung Ethernet in Kbit/s und Mbit/s
- Anzahl der RDP-Sessions der einzelnen Terminal-Server
- Durchsatz und Auslastung der Firewall
- Erreichbarkeit aller Server von außen
- Erreichbarkeit und Durchsatz der Switche

Ein geschütztes Verfahren zur Datensicherung wurde von uns implementiert und ist dokumentiert.

Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden mindestens 10 Tage vorab angekündigt.

In unserem Unternehmen ist es essentiell, Entwicklungs-, Test und Betriebsumgebungen voneinander zu trennen, so dass wir ein besonderes Augenmerk hierauf haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden regelmäßig aktualisiert.

Wir verfügen über eine zentral überwachte und geschützte Ereignisprotokollierung und haben für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre getroffen. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Die Synchronisation unserer Uhren erfolgt zentral mit einer einzigen Referenzzeitquelle.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen.

Es besteht eine Aufstellung unserer technischen Werte und eine geregelte, dokumentierte Handhabung für den Fall einer technischen Schwachstelle, die u.a. unser Patchmanagement mit definierten Verantwortlichkeiten umfasst.

Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral implementiert.

Im Falle einer Auditprüfung unserer Informationssysteme haben wir Maßnahmen festgelegt, die Störungen der Geschäftsprozesse soweit wie möglich minimieren.

1.9 Kommunikationssicherheit

Die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen ist unumgänglich. Daher haben wir dokumentierte Maßnahmen eingesetzt, die unsere Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten.

Wir verfügen über Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen.

Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungs-vereinbarungen ab, die wir regelmäßig überprüfen.

1.10 Anschaffung, Entwicklung und Instandhaltung von Systemen

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme ist. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen. Der Schutz der Transaktionen bei Anwendungsdiensten erfolgt bedarfsgerecht. Zudem haben wir ein Verfahren zur Verwaltung von Systemänderungen eingerichtet, um die Integrität des Systems, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen. Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationssicherheit auch der Kundenanwendungen gibt. Wir verfügen über einen gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Unsere Testdaten werden sorgfältig ausgewählt geschützt und gesteuert.

1.11 Lieferantenbeziehungen

Wir wählen unsere Lieferanten im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes.

Dokumentierte Vereinbarungen sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Die Lieferanten werden verpflichtet, technisch-organisatorische Maßnahmen zu treffen, um dies zu gewährleisten.

Es besteht eine reglementierte und benutzerdefinierte Zugriffsberechtigung auf die für den jeweiligen Lieferanten zwingend benötigten Werte und Daten.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer Lieferanten durch um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

Nach Beendigung des Lieferantenverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Werte zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

1.12 Handhabung von Informationssicherheits- und Datenschutzereignissen

Unser Unternehmen verfügt über einen geregelten dokumentierten Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten. Die Mitarbeiter sind angehalten, sämtliche Datenschutz – und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich regelmäßig geschult. Wir haben ein Meldesystem installiert, das Ereignisse an ein Interventionsteam weitergeleitet, um eine schnelle Reaktion zu gewährleisten. Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet. Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.

Zusammen mit der Geschäftsführung werden regelmäßig Verbesserungsmaßnahmen besprochen und umgesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

1.13 Informationssicherheitsaspekte beim Business Continuity Management

Im Rahmen der Informationssicherheit wird die Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme / Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um. Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien. Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und die Dokumentation der Durchführung entsprechender Tests rundet das Notfallmanagement ab. Alle Server und Storage Systeme sind mit einer mindestens 36-monatigen Herstellergarantie ausgestattet.

1.14 Compliance

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und auf dem neuesten Stand gehalten.

Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen schützen wir Aufzeichnungen und personenbezogene Daten bedarfsgerecht. Jährliche Tätigkeitsberichte des Datenschutzbeauftragten dokumentieren die ergriffenen Maßnahmen.

Wir beachten hierfür die Regelungen Kryptographischer Maßnahmen.

Um den Schutz unserer Informationen und Daten sicher zu stellen, erfolgt regelmäßig eine unabhängige Überprüfung unseres Informationssicherheit- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

2 WEITERE MASSNAHMEN

2.1 Verfahrensverzeichnisse

Aktuelle Verarbeitungsübersicht bzw. Verfahrensverzeichnisse sind vorhanden.

2.2 Rechtsfolgeabschätzungen

Soweit gesetzlich gefordert, werden Verfahren vor ihrer Inbetriebnahme auf Basis vordefinierter Risikokriterien und –stufen identifiziert und den Schutzmaßnahmen gegenübergestellt. Die so getroffenen datenschutzrechtlichen Bewertungen fließen in die Umsetzung der Maßnahmen ein und werden dokumentiert.

2.3 Schulung und Sensibilisierung der Mitarbeiter

Mitarbeiter werden regelmäßig in Fragen des Datenschutzes und der Datensicherheit dokumentiert geschult und sensibilisiert.

3 Regelungen im Unternehmen

Es bestehen unter anderem folgende Informationssicherheits- und Datenschutzregelungen im Unternehmen:

- Richtlinie Betroffenenrechte
- Handbuch Datenschutzmanagementsystem
- Richtlinie Risikoanalyse und -behandlung
- Onboarding Mitarbeiter
- Offboarding Mitarbeiter
- Richtlinie Auftragsverarbeitung
- Richtlinie Berechtigungsvergabe
- Richtlinie Datenschutznotfall
- Kontaktpersonen im Rahmen eines Datenschutznotfalles
- Richtlinie Datenarchivierung und -löschung
- Richtlinie IT-Nutzung
- Übersicht Datenklassifikation und Verarbeitung

Anlage 2 – Zugelassene Subdienstleister

- **Scaleway SAS BP** (Bereitstellung Datencenter)
    - Scaleway SAS BP
      8 rue de la Ville l‘Evêque
      75008 Paris
      Frankreich
- **Billwerk+ Germany GmbH** (Subscription Management, Payment)
    - Billwerk+ Germany GmbH
      Mainzer Landstraße 51
      60329 Frankfurt am Main

Anlage 3 – Weisungsberechtigte Person

Andreas Engl – Head of Digital Health Solutions

E-Mail: a.engl@oped.de

Telefon: 01603677142

Anlage 4 – Datenschutzbeauftragter

c/o activeMind AG Management- und Technologieberatung

Potsdamer Str. 3, 80802 München, Deutschland

E-Mail: datenschutz@oped.de

Anlage 5 – Zertifizierungen

ISO 27001 Zertifikat der OPED GmbH