activeMind.AG

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen	und
der für die Nutzung der Online-Schulung verantwortlichen Stelle	**activeMind AG** **Potsdamer Str. 3** **80802 München**
im Folgenden: **Auftraggeber**	im Folgenden: **Auftragnehmer**

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 in dessen Auftrag verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. 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

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- Bereitstellung und Wartung Online-Schulungs-Portal

Bei der Durchführung des Auftrags kann der Auftragnehmer mit personenbezogenen Daten für die der Auftraggeber verantwortlich ist in Berührung kommen.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) ist im Hauptvertrag für diese Leistung spezifiziert.

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art der Verarbeitung

Die Verarbeitung ist folgender Art: Erfassen, Speicherung, Auslesen, Verwendung, Löschung

3.2 Zweck der Verarbeitung

Die Verarbeitung dient folgendem Zweck:

Zweck der Beauftragung ist die Bereitstellung eines Portals und die Wartung von hierfür notwendigen Datenverarbeitungsanlagen, wobei der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

3.3 Art der Daten

Es werden folgende Daten verarbeitet:

- Name, Vorname, E-Mail-Adresse und zugehöriges Unternehmen des Nutzers
- Kursmetadaten (Fortschritt und Zeitstempel der Registrierung, Lernerfolge)

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Beschäftigte des Auftraggebers

4 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.

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

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, sind schriftlich zur Vertraulichkeit verpflichtet und mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht.

(4) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(5) 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.

(6) 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.

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

5 Sicherheit der Verarbeitung

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird.

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

(4) 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.

(5) Unter Einhaltung der nachstehenden Regelungen ist es dem Auftragnehmer gestattet, Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen zu erlauben. Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch in den Privatwohnungen der Beschäftigten des Auftragnehmers gewährleistet ist. Der Zugang zu Privatwohnungen für Kontrollzwecke stellt der Auftragnehmer vertraglich sicher, soweit ein vom Auftraggeber glaubhaft zu machender dringender Grund für eine

solche Kontrolle besteht. Ein solcher Grund liegt insbesondere dann nicht vor, wenn der Auftragnehmer die Einhaltung der vereinbarten Regelungen nachvollziehbar belegt.

(6) 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) DSGVO.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

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

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

7 Unterauftragsverhältnisse

(1) 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.

(2) 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.

(3) 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.

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

(5) 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.

(6) 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.

8 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. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber glaubhaft zu machenden dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit.

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

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

10 Weisungen

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

(2) 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.

11 Beendigung des Auftrags

Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen.

12 Vergütung

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

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) Im Übrigen gelten die Bestimmungen zur Haftung des Hauptvertrages.

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 und die ausdrückliche Bezugnahme auf diese Vereinbarung 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.

1. Organisation der Informationssicherheit

Die Führungskräfte der activeMind AG 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 des Unternehmens zu reduzieren.

Die activeMind AG verfügt über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutz- und Informationssicherheitsvorfälle rechtzeitig gemeldet werden.

Laufender Kontakt zu speziellen Interessensgruppen wird gepflegt, um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

In Projekten ist Datenschutz und Datensicherheit Bestandteil aller Phasen der Projektmethodik.

Durch die jeweiligen Richtlinien und Prozesse zur Telearbeit und der Nutzung von Mobilgeräten, wird der Datenschutz und die Datensicherheit auch in diesen Bereichen sichergestellt.

2. Personalsicherheit

Mitarbeiter wurden sorgsam ausgewählt und ihre Eignung für ihre Rolle im Unternehmen überprüft. Ihre Verantwortlichkeiten sind in Funktionsbeschreibungen festgelegt und werden regelmäßig abgeglichen, 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. Sie sind sich daher ihrer Verantwortung diesbezüglich bewusst.

Durch einen bestehenden Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses wird sichergestellt, dass personenbezogene Daten geschützt und die Datensicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

3. Verwaltung der Werte

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

Zum Schutz dieser Werte wurden Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Prozesse für den zulässigen Gebrauch der firmeneigenen Werte bestehen. Die Rückgabe erfolgt dokumentiert.

Die 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, werden bestehende Prozesse für die Handhabung der eigenen Werte, insbesondere auch der Wechseldatenträger, entwickelt und umgesetzt. Ein geregelter Prozess zum Transport von Datenträgern, um diese vor unbefugtem Zugriff, Missbrauch oder Verfälschung zu schützen, besteht.

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

4. Zugangssteuerung

Es existieren geregelte und bestehende Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogene 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 bestehenden und restriktiven Berechtigungskonzepts vergeben. Der Zugang zu Netzwerken und Netzwerkdiensten ist 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 De-Registrierung von Benutzern, der die Zuordnung von Zugangsrechten ermöglicht.

Administrative Rechte werden nur eingeschränkt und gesteuert erteilt.

Ein geregelter Prozess über den Umgang mit Passwörtern besteht. Der Ist- und Soll-Zustand von Benutzerzugangsrechten wird regelmäßig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Der Zugriff auf Daten wird bedarfsgerecht eingeschränkt und der Zugang auf Systeme und Anwendungen wird durch ein sicheres Anmeldeverfahren gesteuert. Es wird ein System zur Nutzung sicherer und starker Kennwörter verwendet.

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

5. Kryptographie

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

6. Physische und umgebungsbezogene Sicherheit

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

Standort Potsdamer Straße 3, 80802 München; Standort Leopoldstraße 182, 80804 München & Standort Kurfürstendamm 56, 10707 Berlin

- Gebäude und Sicherheitsbereiche können selbständig nur von berechtigten Personen betreten werden
- IT-Räume sind eigens gesondert gesichert.
- Besucher und Lieferanten können das Gebäude nur über den Haupteingang betreten. Sie müssen durch einen Berechtigten eingelassen werden. Sie werden innerhalb des Gebäudes von Mitarbeitern begleitet.
- Im Rechenzentrum wird kein externes Personal eingesetzt.
- Externen Personen eingeräumte Zutrittsrechte sind auf das notwendige Minimum zu beschränken.

7. Betriebssicherheit

Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen, sind vorhanden. 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
- Wesentliche Dienste und Status aller virtuellen Maschinen
- Fehlerhafte Anmeldeversuche
- Speicherbelegung der Storages und Hauptspeicher
- Durchsatz und Auslastung der Firewall
- Erreichbarkeit aller Server von außen

Ein geschütztes Verfahren zur Datensicherung ist implementiert.

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

Eine überwachte und geschützte Ereignisprotokollierung ist für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre vorhanden. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Die Synchronisation firmeninterner Uhren erfolgt zentral mit einer Referenzzeitquelle.

Ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen im Unternehmen ist verfügbar.

Es besteht eine Aufstellung der technischen Werte und eine geregelte Handhabung für den Fall einer technischen Schwachstelle, die u.a. das Patch-Management mit definierten Verantwortlichkeiten umfasst.

Regelungen für die Einschränkungen von Softwareinstallationen sind zentral implementiert.

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

8. Kommunikationssicherheit

Als beratendes Unternehmen im Bereich Datenschutz und Datensicherheit ist die Sicherheit der in eignen Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen unumgänglich. Daher werden bestehende Maßnahmen eingesetzt, die die Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt.

Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen sind verfügbar.

Die elektronische Nachrichtenübermittlung wird angemessen geschützt. Unter anderem bestehen Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Zum Schutz der firmeneigenen Daten, werden bedarfsgerechte Vertraulichkeits- oder Geheimhaltungsvereinbarungen abgeschlossen, die regelmäßig überprüft werden.

9. Anschaffung, Entwicklung und Instandhaltung von Systemen

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus der eignen 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 wurde 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. Ein gesteuerter Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme ist vorhanden.

10. Lieferantenbeziehungen

Lieferanten werden im Vorfeld sorgsam ausgewählt und ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes überprüft.

Bestehende Prozesse sichern den Schutz und die Geheimhaltung unternehmenseigener 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 Zustimmung der activeMind AG beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig wird eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen eigener Lieferanten durchgeführt, um das vereinbarte Niveau aufrechtzuerhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

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

11. Handhabung von Informationssicherheitsvorfällen

Die activeMind AG verfügt über einen geregelten bestehenden 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. Ein Meldesystem ist 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.

12. Informationssicherheitsaspekte beim Business Continuity Management

Im Rahmen der Informationssicherheit wird die Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen werden die technischen und organisatorischen Vorgaben, wie redundante Systeme / Anbindungen oder entsprechende Planungen abgeleitet und diese konsequent und gesteuert umgesetzt. Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte Notfallszenarien. Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und bestehende Prozesse der Durchführung entsprechender Tests rundet das Notfallmanagement ab.

13. Compliance

Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens werden 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.

Hierfür werden die Regelungen kryptographischer Maßnahmen beachtet.

Um den Schutz der Informationen und Daten sicherzustellen, erfolgt regelmäßig eine unabhängige Überprüfung des unternehmenseigenen Informationssicherheit- und Datenschutzniveaus, der Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

Anlage 2 – Zugelassene Subdienstleister

Firma	Anschrift	Auftragsinhalt
Global Access Internet Services GmbH	Potsdamer Straße 3, 80802 München	ISO 27001-zertifiziertes Rechenzentrum
Midland-IT GmbH	Marienstraße 76, 32427 Minden	IT-Support
neudenken Strategieagentur	Friedrichstraße 123, 10117 Berlin	Bereitstellung von Dienstleistungen bezüglich der technischen Webseitengestaltung und –verwaltung
JKDV-Systeme GmbH	Bahnstraße 34, 25451 Quickborn	Bereitstellung von Dienstleistungen bezüglich der technischen Webseitengestaltung und –verwaltung

Anlage 3 – Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutz-verletzungen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

- Klaus Foitzick, activeMind AG
- Michael Plankemann, activeMind AG
- Dr. Evelyne Sørensen, activeMind AG

Anlage 4 – Datenschutzbeauftragter

Derzeit ist als interner Datenschutzbeauftragter beim Auftragnehmer bestellt:

Datenschutzbeauftragter der activeMind AG
Telefon: +49 (0)89 / 91 92 94 - 900
E-Mail: datenschutz@activemind.de

Anlage 5 –Datenschutzbeauftragter

TÜV PROFI CERT

ZERTIFIKAT

für das Managementsystem nach

ISO/IEC 27001:2013

Der Nachweis der regelkonformen Anwendung wurde erbracht
und wird gemäß TÜV PROFiCERT-Verfahren bescheinigt für

activeMind.AG

activeMind AG Management- und Technologieberatung
activeMind.legal Rechtsanwaltsgesellschaft mbH
Potsdamer Straße 3
80802 München / Deutschland
inklusive der Standorte gemäß Anhang

Geltungsbereich:

Stellung von Datenschutz-, Informationssicherheitsbeauftragten
und EU Repräsentanten;
Aufbau und Prüfung von Datenschutz- und
Informationssicherheitsmanagementsystemen;
Hosting und Betrieb von Kundenportalen

Statement of Applicability (SoA): Version 4 / 2019-02-04

Zertifikat-Registrier-Nr. **73 121 6356** Zertifikat gültig von 2019-06-27 bis **2022-06-26**

Auditbericht-Nr. 4348 9948

DAkkS Deutsche Akkreditierungsstelle D-ZM 14137-01-00

TÜV HESSEN

Darmstadt, 2019-06-27
Zertifizierungsstelle des TÜV Hessen
– Der Zertifizierungsstellenleiter –

SEITE 1 VON 6.
Diese Zertifizierung wurde gemäß TÜV PROFICERT-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.proficert.com. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Robert-Bosch-Straße 16, D-64293 Darmstadt, Tel. +49 6151/600331 Rev-DE-1711

TÜV PROFI CERT

ZERTIFIKAT

für das Managementsystem nach

DIN EN ISO 9001:2015

Der Nachweis der regelkonformen Anwendung wurde erbracht
und wird gemäß TÜV PROFiCERT-Verfahren bescheinigt für

ActiveMind AG Management- und Technologieberatung
Potsdamer Str. 3, 80802 München / Deutschland

mit dem Standort:

activeMind.AG

activeMind AG Management- und Technologieberatung
Potsdamer Straße 3
80802 München / Deutschland

Geltungsbereich:

Stellung von Datenschutz-, Informationssicherheitsbeauftragten;
Aufbau und Prüfung von Datenschutz- und
Informationssicherheitsmanagementsystemen;
Hosting und Betrieb von Kundenportalen

Zertifikat-Registrier-Nr. **73 100 6356-1** Zertifikat gültig von 2019-05-02 bis **2022-05-01**

Auditbericht-Nr. 4348 9948

DAkkS Deutsche Akkreditierungsstelle D-ZM-14137-01-00

TÜV HESSEN

Darmstadt, 2019-05-02
Zertifizierungsstelle des TÜV Hessen
– Der Zertifizierungsstellenleiter –

SEITE 3. Nur gültig in Verbindung mit dem Hauptzertifikat 73 100 6356.
Diese Zertifizierung wurde gemäß TÜV PROFiCERT-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.proficert.com. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Robert-Bosch-Straße 16, D-64293 Darmstadt, Tel. +49 6151/600331 Rev-DE-1711