Datenschutzerklärung GAIA Online-Programme

Datenschutz hat einen besonders hohen Stellenwert für die Geschäftsleitung. Ist die Verarbeitung personenbezogener Daten erforderlich und besteht für eine solche Verarbeitung keine gesetzliche Grundlage, holen wir generell eine Einwilligung der betroffenen Person ein.

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rechtsgebiet der EU und stets im Einklang mit der EU-Datenschutz-Grundverordnung (DS-GVO) und in Übereinstimmung mit dem deutschen Bundesdatenschutzgesetz und – wenn anwendbar - dem “Health Insurance Portability and Accountability Act” (HIPAA). Mittels dieser Datenschutzerklärung möchte unser Unternehmen die Öffentlichkeit über Art, Umfang und Zweck der von uns erhobenen, genutzten und verarbeiteten personenbezogenen Daten informieren. Ferner werden betroffene Personen mittels dieser Datenschutzerklärung über die ihnen zustehenden Rechte aufgeklärt.

Wir haben als für die Verarbeitung Verantwortlicher zahlreiche technische und organisatorische Maßnahmen umgesetzt, um einen möglichst lückenlosen Schutz der verarbeiteten personenbezogenen Daten sicherzustellen.

Name und Anschrift des für die Verarbeitung Verantwortlichen

Verantwortlicher im Sinne der Datenschutz-Grundverordnung, sonstiger in den Mitgliedstaaten der Europäischen Union geltenden Datenschutzgesetze und anderer Bestimmungen mit datenschutzrechtlichem Charakter, wie zum Beispiel HIPAA, ist die:

GAIA AG
Hans-Henny-Jahnn-Weg 53
22085 Hamburg, Deutschland

Kontakt zum Datenschutzbeauftragten: privacy@gaia-group.com

Cookies

Wir verwenden keine Cookies.

Erfassung von allgemeinen Daten und Informationen

Die Internetseite erfasst mit jedem Aufruf durch eine betroffene Person oder ein automatisiertes System eine Reihe von allgemeinen Daten und Informationen. Diese allgemeinen Daten und Informationen werden in den Logfiles des Servers temporär gespeichert. Erfasst werden können die (1) verwendeten Browsertypen und Versionen, (2) das vom zugreifenden System verwendete Betriebssystem, (3) die Internetseite, von welcher ein zugreifendes System auf unsere Internetseite gelangt (sogenannte Referrer), (4) die Unterwebseiten, welche über ein zugreifendes System auf unserer Internetseite angesteuert werden, (5) das Datum und die Uhrzeit eines Zugriffs auf die Internetseite, (6) eine Internet-Protokoll-Adresse (IP-Adresse) und (7) sonstige ähnliche Daten und Informationen, die der Gefahrenabwehr im Falle von Angriffen auf unsere informationstechnologischen Systeme dienen.

Bei der Nutzung dieser allgemeinen Daten und Informationen ziehen wir keine Rückschlüsse auf die betroffene Person. Diese Informationen werden vielmehr benötigt, um (1) die Inhalte unserer Internetseite korrekt auszuliefern, (2) die Inhalte unserer Internetseite zu optimieren, (3) die dauerhafte

Funktionsfähigkeit unserer informationstechnologischen Systeme und der Technik unserer Internetseite zu gewährleisten sowie (4) um Strafverfolgungsbehörden im Falle eines Cyberangriffes die zur Strafverfolgung notwendigen Informationen bereitzustellen.

Erfassung von personenbezogenen Daten und Gesundheitsdaten

Zweck der Datenverarbeitung ist die Bereitstellung des Online-Programms attexis, das therapeutische Techniken und Übungen vermittelt, die auf evidenzbasierten psychologisch-psychotherapeutischen Therapieverfahren beruhen und die für Patienten mit ADHS (Aufmerksamkeitsdefizit-Hyperaktivitätsstörung) geeignet sind, diese beim Management ihrer ADHS zu unterstützen.
Bei der Registrierung für attexis werden die zur Registrierung erforderlichen Daten (E-Mail-Adresse, Passwort, Anrede) erhoben und gespeichert, damit attexis genutzt werden kann. Optional werden Mobilnummer und Aufenthaltsland erhoben, welche für die freiwillige Nutzung des SMS-Services notwendig sind. Im Rahmen des weiteren Programmverlaufs werden zusätzlich regelmäßig (wöchentlich) Gesundheitsdaten via freiwilliger Selbstauskünfte erhoben, um die Inhalte von attexis thematisch auf Ihre Bedürfnisse anzupassen und Ihnen zur Selbstbeobachtung zu dienen. Diese Fragen bedienen die Themen Herausforderungen des Alltags, Umgang mit diesen Herausforderungen, allgemeine Lebensweise, Selbstreflexion sowie künftige Ziele.
Betroffene Personen in Deutschland können eine Integration einrichten, um sich sicher über die GesundheitsID in attexis einzuloggen. Um diese Integration zu ermöglichen, wird die deutsche Krankenversicherungsnummer (KVNR) der betroffenen Person vom Verantwortlichen gespeichert, solange die Integration aktiv bleibt. Sobald die Integration mit der GesundheitsID hergestellt wurde, hat die betroffene Person auch die Möglichkeit, ein Datenpaket mit den oben genannten Gesundheits- und personenbezogenen Daten über die Option auf der Seite „Einstellungen“ an ihre deutsche elektronische Patientenakte (ePA) zu senden. Damit die Übertragung in die ePA funktioniert, muss die Zustimmung für die Anwendung direkt in der ePA erteilt werden. Diese Zustimmung kann jederzeit direkt in der ePA widerrufen werden.

Alle Angaben werden ausschließlich genutzt, um alle im Zusammenhang mit der Nutzung dieses Online-Programms stehenden Aktionen durchführen zu können und für Sie nützliche Informationen zu vermitteln.

Der für die Verarbeitung Verantwortliche kann die Weitergabe an einen oder mehrere Auftragsverarbeiter veranlassen, der die personenbezogenen Daten ebenfalls ausschließlich für eine interne Verwendung, die dem für die Verarbeitung Verantwortlichen zuzurechnen ist, nutzt. Um die effiziente Zustellung wichtiger Mitteilungen zu ermöglichen, kann der Verantwortliche die E-Mail-Adresse und Mobilnummer der betroffenen Person an einen Drittanbieter weitergeben, der im Auftrag des Verantwortlichen für die Zustellung von Nachrichten verantwortlich ist. Darüber hinaus kann die E-Mail-Adresse der betroffenen Person an einen Anbieter von Ticketing-Software weitergegeben werden, um bei der Lösung von Supportanfragen zu helfen. Die Integrationen für die GesundheitsID und die ePA werden ebenfalls über Drittanbieter verwaltet, die die Kommunikation mit der deutschen Telematikinfrastruktur ermöglichen. Diese Auftragsverarbeiter sind zur Vertraulichkeit verpflichtet und dürfen die Daten ausschließlich für die angegebenen Zwecke gemäß den geltenden Datenschutzgesetzen verwenden.

Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten

Die Anwendung wird ausschließlich in ISO 27001 zertifizierten Rechenzentren in Deutschland betrieben. Das Rechenzentrum ist gegen unbefugten Zugriff auf die Anlage, Unterbrechung der

Stromversorgung, unbefugten Datenzugriff und Beeinträchtigung der Verfügbarkeit geschützt, dies entspricht den Anforderungen der DSGVO.
Ein Qualitätsmanagementsystem (QMS) nach ISO 13485 wurde von GAIA implementiert und zertifiziert. Im Rahmen des QMS wird die Absicherung möglicher Risiken im Bereich „Cyber Security“ umgesetzt. Mindestens einmal jährlich wird die Software- und Infrastruktursicherheit durch externe Spezialisten für Penetrationstests überprüft. Darüber hinaus hat GAIA ein nach ISO 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS) implementiert, um die Qualität der internen Prozesse in Bezug auf die Informationssicherheit sicherzustellen.
GAIA erhebt nur die minimale Menge an personenbezogenen Daten, die zur Erbringung ihrer Dienstleistungen erforderlich ist. Die gesammelten persönlichen Benutzerdaten werden niemals an Dritte weitergegeben oder anderweitig mit solchen geteilt. Bei der Übertragung wird der gesamte Datenverkehr während des administrativen Zugriffs und des Zugriffs durch Endbenutzer TLS-verschlüsselt, sodass ein Abfangen und Verändern der Daten durch Dritte nicht möglich ist.
Darüber hinaus hat GAIA eine Reihe zusätzlicher Maßnahmen implementiert, die dem Nutzer einen zusätzlichen Schutz seiner personenbezogenen Daten bieten sollen:

- Ein Session-Timeout ist implementiert
- Es findet ein Double-Opt-In-Verfahren statt. Dadurch wird überprüft, ob eine angegebene E-Mail-Adresse auch dem Benutzer gehört.
- Eine stündliche Datensicherung wird durchgeführt. Das entsprechende „Disaster Recovery“ wird mindestens monatlich getestet.
- Gaia-Server werden auf Anomalien und Cyberangriffe überwacht und sind durch eine Firewall geschützt.
- Ein „Passwort vergessen“-Prozess ist implementiert.
- Die persönlichen Benutzerdaten werden niemals außerhalb einer sicheren Serverumgebung im Rechenzentrum gespeichert.
- Alle Anbieter und Softwarebibliotheken werden im Rahmen unseres ISMS geprüft.

Wir weisen darauf hin, dass Sie für das Einloggen und die Nutzung des Programms aus einer sicheren Umgebung selbst verantwortlich sind und die Nutzung des Programms in einer potenziell unsicheren Umgebung mit Sicherheitsrisiken einhergeht, die durch die GAIA AG nicht vollständig adressiert werden können.

Löschung und Sperrung von personenbezogenen Daten und Gesundheitsdaten

Nach Ende der Programmnutzung (Nutzungszeitraum 90 Tage) werden alle personenbezogenen Daten automatisch und unverzüglich gelöscht.

Sie können uns jederzeit mit der Löschung Ihrer Daten beauftragen, indem Sie das Kontaktformular über den “Hilfe & Kontakt”-Menüpunkt nutzen und den entsprechenden vorgefertigten Betreff zum “Widerruf erteilter Einwilligungen” auswählen. Das Kontaktformular wird automatisch mit dem entsprechenden Text zur Aufforderung der Löschung Ihrer Daten gefüllt und kann von Ihnen ohne weiteren Aufwand abgesendet werden. Falls Sie die Einwilligung in die Verarbeitung Ihrer personenbezogenen Daten widerrufen, werden diese unverzüglich gelöscht, und Sie haben dann keine Möglichkeit mehr, das Programm zu nutzen, da der Zugang gesperrt wird.

Wenn Sie Ihre Daten vor dem Löschen exportieren möchten, wählen Sie dazu bitte den Menüpunkt “Einstellungen” aus und klicken unten auf der Seite auf “Download”. Wenn der Zugang zu attexis gesperrt und Ihre personenbezogenen Daten gelöscht sind, ist kein Export Ihrer Daten mehr möglich.

Rechte der betroffenen Person

a) Recht auf Bestätigung

Jede betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber eingeräumte Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden.

b) Recht auf Auskunft

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, jederzeit von dem für die Verarbeitung Verantwortlichen unentgeltliche Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten und eine Kopie dieser Auskunft zu erhalten.

Ferner steht der betroffenen Person ein Auskunftsrecht darüber zu, ob personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt wurden. Sofern dies der Fall ist, so steht der betroffenen Person im Übrigen das Recht zu, Auskunft über die geeigneten Garantien im Zusammenhang mit der Übermittlung zu erhalten.

Des Weiteren steht der betroffenen Person ein Beschwerderecht bei einer Aufsichtsbehörde zu.

c) Recht auf Berichtigung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Ferner steht der betroffenen Person das Recht zu, unter Berücksichtigung der Zwecke der Verarbeitung, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

d) Recht auf Löschung (Recht auf Vergessen werden)

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe zutrifft und soweit die Verarbeitung nicht erforderlich ist:

- Die personenbezogenen Daten wurden für solche Zwecke erhoben oder auf sonstige Weise verarbeitet, für welche sie nicht mehr notwendig sind.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 Buchstabe a DS-GVO oder Art. 9 Abs. 2 Buchstabe a DS-GVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

e) Recht auf Einschränkung der Verarbeitung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.
- Die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten.
- Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person hat Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DS-GVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

f) Recht auf Mitteilung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht auf Mitteilung sowie Benachrichtigung im Rahmen der Berichtigung, Löschung oder Einschränkung gegenüber Empfängern.

g) Recht auf Datenübertragbarkeit

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die sie betreffenden personenbezogenen Daten, welche durch die betroffene Person einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

h) Recht auf Widerspruch

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f DS-GVO erfolgt, Widerspruch einzulegen.

Wir verarbeiten die personenbezogenen Daten im Falle des Widerspruchs nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

i) Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, sofern die Entscheidung (1) nicht für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, oder (2) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder (3) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

j) Recht auf Widerruf einer datenschutzrechtlichen Einwilligung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, eine Einwilligung zur Verarbeitung personenbezogener Daten jederzeit zu widerrufen.

Studien und Forschungszwecke

Haben Sie Ihren Zugangsschlüssel als Teil einer wissenschaftlichen Studie erhalten und haben Sie der Studieneinwilligungserklärung zugestimmt, erlauben Sie eine pseudonymisierte Datenweitergabe an Ihr verantwortliches Studienteam sowie an andere wissenschaftliche Kooperationspartner, die den Nutzen des Programms evaluieren.

Die Speicherung erfolgt immer nach den gesetzlichen Datenschutzbestimmungen.

Vertriebspartner

Sollte Ihnen der Zugang zu diesem Produkt durch einen Vertriebspartner oder andere Dritte ermöglicht worden sein, so erhalten diese zu keinem Zeitpunkt Einblick in bzw. Zugriff auf Ihre Daten. Dies gilt nicht, wenn der Kundensupport zur Beantwortung von Benutzeranfragen (First Level Support) durch den Vertriebspartner bereitgestellt wird.

Sollte der First Level Support in Ausnahmefällen nicht direkt von GAIA bereitgestellt werden, finden Sie weitere Informationen in Kapitel 4 der Allgemeinen Geschäftsbedingungen.

Rechtsgrundlage der Verarbeitung

Ist die Verarbeitung personenbezogener Daten und Gesundheitsdaten zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich, wie dies beispielsweise bei Verarbeitungsvorgängen der Fall ist, die für eine Lieferung von Waren oder die Erbringung einer sonstigen Leistung oder Gegenleistung notwendig sind, so beruht die Verarbeitung auf Art. 6 I lit.a und b DS-GVO sowie Art. 9 II lit.a sowie auf der entsprechenden Regelung im HIPAA.

Dies trifft auf uns zu, da der Nutzer während der Registrierung mit uns eine Nutzungsvereinbarung (AGB) eingeht.

Dauer, für die die personenbezogenen Daten und Gesundheitsdaten gespeichert werden

Das Kriterium für die Dauer der Speicherung von personenbezogenen Daten ist die jeweilige gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

Haben Sie Ihren Zugangsschlüssel im Rahmen einer DiGA Verordnung erhalten, ist die Speicherdauer von personenbezogenen Daten auf 90 Tage begrenzt.

Bestehen einer automatisierten Entscheidungsfindung

Als verantwortungsbewusstes Unternehmen verzichten wir auf eine automatische Entscheidungsfindung oder ein Profiling.

21.11.2024