Öffentliches Dokument

Datenschutzbestimmungen der Frieda-App

Version: 1.3.0
Datum: 08.10.2025

Erstellt im Auftrag von
Frieda Health GmbH
Cremon 11
20457 Hamburg

Erstellt durch
QuR.digital GmbH
Große Elbstraße 42
22767 Hamburg

Öffentliches Dokument

Inhaltsverzeichnis

Allgemeine Hinweise

Wir nehmen den Schutz Ihrer personenbezogenen Daten (nachfolgend „Daten“ genannt) ernst und halten uns an die geltenden Datenschutzgesetze.

Mit dieser Datenschutzerklärung kommen wir unseren Informationspflichten aus Art. 12 ff. der Datenschutz-Grundverordnung (nachfolgend „DSGVO“ genannt) nach. Diese soll Ihnen einen Überblick darüber geben, wie wir mit Ihren personenbezogenen Daten umgehen, die im Rahmen der Nutzung unseres Leistungsangebotes verarbeitet werden.

Unser Leistungsangebot umfasst die Vermittlung gynäkologischer Sprechstunden, welche sich auf Beschwerden in den Wechseljahren fokussieren, die Bereitstellung unserer digitalen Plattform, sowie telemedizinischer Software, um Patientinnen telemedizinischen Leistungen aus dem Fachgebiet der Gynäkologie mit Fokus auf Wechseljahresbeschwerden anbieten können. Das Leistungsangebot umfasst neben der Frieda Health-Webplattform auch die verschreibungspflichtige App Frieda Menova DiGA (nachfolgend “Frieda-App” genannt) mit dem Fokus auf Symptombewältigung in den Wechseljahren. Die App enthält einen 12-wöchigen Kurs zur Erlernung bewährter Strategien für weniger Hitzewallungen, besseren Schlaf und mehr innere Ruhe, Gelassenheit, Selbstfürsorge und einen besseren Umgang mit emotionalen Stress. Die Kursinhalte umfassen psychoedukative Texte, Videos und Übungen.

Bitte lesen Sie unsere Datenschutzerklärung im Zusammenhang mit unseren Allgemeinen Geschäftsbedingungen.

Begriffsbestimmungen

- „Verantwortlicher“ ist gemäß Art. 4 Nr.7 DSGVO derjenige, der über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheidet. Er bestimmt vor allem was, wie und wofür verarbeitet wird. Er ist für die Verarbeitung verantwortlich und hat sicherzustellen, dass die datenschutzrechtlichen Vorschriften eingehalten werden.
- „Auftragsverarbeiter“ ist gemäß Art. 4 Nr.8 DSGVO derjenige, der für den Verantwortlichen tätig wird und in dessen Auftrag personenbezogene Daten verarbeitet.
- „Personenbezogene Daten“ sind gemäß Art. 4 Nr.1 DSGVO alle Informationen, die sich einer unmittelbar oder mittelbar bestimmbaren natürlichen Person („betroffene Person“) zuordnen lassen

- „Verarbeitung“ meint gemäß Art. 4 Nr.2 DSGVO alle möglichen Arten der Datenverarbeitung. Darunter insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Verknüpfen, Einschränken, Löschen oder Vernichten von personenbezogenen Daten.
- „Betroffene Person“ ist gemäß Art. 4 Nr.1 DSGVO diejenige natürliche Person, der sich die durch den Verantwortlichen verarbeiteten Daten unmittelbar oder mittelbar zuordnen lassen.
- „Empfänger“ ist gemäß Art. 4 Nr.9 DSGVO derjenige, dem personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich um einen Dritten handelt oder nicht.
- „Dritter“ ist gemäß Art. 4 Nr.10 DSGVO jeder, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters dazu befugt sind, die personenbezogenen Daten zu verarbeiten.
- „Besondere Kategorien personenbezogener Daten“ sind gemäß Art. 9 Abs.1 DSGVO insbesondere auch Gesundheitsdaten der betroffenen Person. Diese Daten weisen einen höheren Schutzbedarf auf.
- „Gesundheitsdaten“ sind gemäß Art. 4 Nr.15 DSGVO solche personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit der betroffenen Person beziehen und aus denen Informationen über den Gesundheitszustand der betroffenen Person hervorgehen.
- „Einwilligung“ meint gemäß Art. 4 Nr.11 DSGVO jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung (z.B. das Setzen eines Hakens in einer hierfür vorgesehenen Checkbox), mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist.
- „Pseudonymisierung" bedeutet gemäß Art. 4 Nr.5 DSGVO, dass personenbezogene Daten so verarbeitet werden, dass sie nicht mehr einer spezifischen Person zugeordnet werden können, ohne zusätzliche Informationen. Diese zusätzlichen Informationen müssen separat aufbewahrt werden und Maßnahmen müssen ergriffen werden, um sicherzustellen, dass die Daten nicht mehr einer identifizierten oder identifizierbaren Person zugeordnet werden können.
- „Anonymisierung" ist gemäß DIN EN ISO 25237 der Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei

unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt.

Angaben zum Verantwortlichen

Für die Datenverarbeitung im Rahmen des Leistungsangebotes verantwortlich im Sinne von Art. 4 Nr.7 DSGVO ist als Anbieter des Leistungsangebotes die

Frieda Health GmbH (nachfolgend „Frieda Health“)
Cremon 11
20457 Hamburg
Deutschland

vertreten durch die Geschäftsführung.

Fragen zum Datenschutz

Bei Fragen im Zusammenhang mit der Verarbeitung Ihrer Daten sowie bezüglich der Wahrnehmung Ihrer Rechte als betroffene Person im Sinne der DSGVO, stehen wir Ihnen – als Verantwortlicher – jederzeit per E-Mail an hello@frieda.health zur Verfügung. Dies gilt auch, wenn Ihnen ein im Rahmen dieser Datenschutzerklärung verwendeter Begriff unklar sein sollte.

Alternativ können Sie sich mit Anfragen auch an unseren Datenschutzbeauftragten (DSB) wenden. Diesen können Sie unter den folgenden Kontaktdaten erreichen:

Katharina Böck
QuR.digital GmbH
Große Elbstraße 42
22767 Hamburg

Bitte beachten Sie, dass wir im Falle einer Geltendmachung von Betroffenenrechten (z.B. Auskunftsersuchen) zunächst Ihre Identität durch ein hierfür geeignetes Verfahren sicherstellen müssen.

Im Falle von Fragen zur oder technischen Problemen mit unserer App, können Sie sich per E-Mail an hello@frieda.health wenden.

Hinweise zu den erforderlichen datenschutzrechtlichen Einwilligungen

Im Rahmen der App-Nutzung ist Ihre Einwilligung zu bestimmten Datenverarbeitungen erforderlich. Details entnehmen Sie bitte der folgenden Übersicht:

Einwilligung	Zweck der Verarbeitung / rechtliche Grundlage	Konsequenz bei Nichterteilung oder Widerruf
AGB	Nutzung der App auf Grundlage unserer Allgemeinen Geschäftsbedingungen (Art. 6 Abs. 1 lit. b DSGVO)	Eine Nutzung der App ist ohne Zustimmung zu den AGB nicht möglich; das Nutzerkonto wird deaktiviert bzw. gelöscht.
Widerrufsbelehrung	Erfüllung gesetzlicher Informationspflichten im Rahmen von Fernabsatzverträgen (§ 312g BGB i.V.m. Art. 246a EGBGB)	Ohne Bestätigung ist eine vertragskonforme Nutzung nicht möglich; das Nutzerkonto wird deaktiviert bzw. gelöscht.
Kontraindikationen*	Prüfung, ob medizinische Ausschlussgründe einer App-Nutzung entgegenstehen (Art. 6 Abs. 1 lit. a, ggf. Art. 9 Abs. 2 lit. a DSGVO)	Die Nutzung der App ist ohne diese Angabe nicht zulässig; das Nutzerkonto wird deaktiviert bzw. gelöscht.
Tracking und Datenanalyse (optional)	Erhebung und Auswertung von Nutzungsdaten zur Verbesserung der App-Qualität und Nutzerfreundlichkeit (Art. 6 Abs. 1 lit. a DSGVO)	Die App bleibt bei Verweigerung der Einwilligung vollumfänglich funktionsfähig.

*Weiterführende Informationen zu Kontraindikationen finden Sie in der Gebrauchsanweisung unter: https://www.frieda.health/gebrauchsanweisung.

Hinweise zur Datensicherheit

Um den bestmöglichen Schutz Ihrer Daten zu gewährleisten, werde diese während des Transports mit einer Secure-Socket-Layer-Verschlüsselung (SSL-Verschlüsselung) im Verbund mit einer Transport-Layer-Security-Verschlüsselung (TLS-Verschlüsselung) gesichert. Diese Form der Verschlüsselung sorgt dafür, dass die Daten nicht während der Übertragung von unbefugten Dritten ausgelesen, umgeleitet oder verändert werden können.

Soweit Ihre Daten von uns gespeichert werden, erfolgt diese Speicherung ausschließlich in entsprechend sicherheitszertifizierten Rechenzentren innerhalb der Europäischen Union (EU) im Geltungsbereich der DSGVO. Dabei behalten wir uns ausdrücklich das Recht vor, für die Speicherung und Verarbeitung Ihrer Daten externe Dienstleister einzubinden, die jedoch ausschließlich im Auftrag und gemäß den Weisungen von uns tätig werden (Auftragsverarbeiter). Die eingesetzten Auftragsverarbeiter werden von uns vertraglich dazu verpflichtet, solche technischen und organisatorischen Maßnahmen (TOMs) zu ergreifen, die nach dem aktuellen Stand der Technik dazu geeignet sind, eine datenschutzkonforme Verarbeitung Ihrer Daten zu gewährleisten.

In keinem Fall werden Ihre Daten von uns oder einem eingesetzten Auftragsverarbeiter ohne gesetzliche Grundlage an Dritte weitergegeben oder veräußert.

Datenübermittlung an Drittländer

Wir setzen unter Umständen solche Dienstleister als Auftragsverarbeiter ein, die ihren Geschäftssitz in einem Drittland unterhalten oder Teil einer internationalen Organisation sind, die ihren Geschäftssitz in einem Drittland unterhält. Unter einem Drittland ist im Kontext der DSGVO ein Land zu verstehen, das kein Mitglied der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) ist und damit nicht unter den Regelungseinfluss der DSGVO fällt. Diese Drittländer haben gemeinsam, dass diese mitunter über ein eigenes Datenschutzrecht verfügen, welches inhaltlich jedoch unter dem Schutzniveau der DSGVO liegen kann. Vor diesem Hintergrund sieht Art. 44 DSGVO vor, dass die Übermittlung von Daten an Drittländer nur unter bestimmten gesetzlichen Voraussetzungen zulässig ist.

Im Regelfall wird die Zulässigkeit der Datenübermittlung in Drittländer gemäß Art. 45 DSGVO auf einen Angemessenheitsbeschluss zwischen der EU-Kommission und dem betreffenden Drittland gestützt. Das Vorliegen eines Angemessenheitsbeschlusses bringt zum Ausdruck, dass das in dem betreffenden Drittland geltende Datenschutzrecht ein zur DSGVO vergleichbares Schutzniveau für Ihre personenbezogenen Daten aufweist. Sofern kein solcher Angemessenheitsbeschluss vorliegt, wird Datenübermittlung gemäß Art. 46 Abs.2 Buchstabe c) DSGVO alternativ auf den Abschluss eines Vertrages zwischen uns und dem entsprechenden Dienstleister auf Grundlage der von der EU-Kommission erlassenen Standardvertragsklauseln gestützt. Diese Vertragsklauseln liefern eine hinreichende Garantie seitens des jeweiligen Dienstleisters auch im Hinblick auf die Durchsetzbarkeit der von der DSGVO vorgesehenen Betroffenenrechte.

Sie werden von uns im Rahmen dieser Datenschutzerklärung ausdrücklich darauf hingewiesen, wenn ein Dienstleister einen solchen Drittlandsbezug aufweist. In diesem Fall stimmen Sie mit der Erteilung Ihrer Einwilligung zu, dass Ihre personenbezogenen Daten an ein solches Unternehmen übermittelt werden.

Ihre Rechte

Als von der Datenverarbeitung “betroffene Person” im Sinne von Art. 4 Nr. 1 DSGVO stehen Ihnen bestimmte, unabdingbare Rechte zu (Betroffenenrechte). Dabei sind wir zur Gewährleistung dieser Betroffenenrechte verpflichtet und müssen auch eingesetzte Auftragsverarbeiter vertraglich dazu verpflichten, uns bei der Umsetzung dieser Rechte bestmöglich zu unterstützen. Insoweit stehen Ihnen die folgenden Betroffenenrechte zu:

- Recht auf Auskunft (Artikel 15 DSGVO): Sie haben das Recht, von uns Informationen darüber zu erhalten, ob wir personenbezogene Daten von Ihnen verarbeiten und falls ja, welche Daten das sind und zu welchem Zweck die Verarbeitung erfolgt.
- Recht auf Berichtigung (Artikel 16 DSGVO): Sie haben das Recht, unrichtige oder unvollständige personenbezogene Daten, die wir von Ihnen gespeichert haben, korrigieren zu lassen.
- Recht auf Löschung (Artikel 17 DSGVO): Sie haben unter bestimmten Umständen das Recht, von uns die Löschung Ihrer personenbezogenen Daten zu verlangen. Dieses Recht besteht beispielsweise, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind oder wenn Sie Ihre Einwilligung widerrufen haben.

- Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO): Sie haben unter bestimmten Umständen das Recht, die weitere Verarbeitung Ihrer personenbezogenen Daten einzuschränken. Dieses Recht besteht beispielsweise, wenn Sie die Richtigkeit der Daten bestreiten oder die Verarbeitung unrechtmäßig ist.
- Recht auf Datenübertragbarkeit (Artikel 20 DSGVO): Sie haben das Recht, von uns eine Kopie Ihrer personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie können diese Daten auch an einen anderen Verantwortlichen übermitteln lassen, sofern dies technisch möglich ist.
- Recht auf Widerspruch (Artikel 21 DSGVO): Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung Ihrer personenbezogenen Daten Widerspruch einzulegen. Wir werden Ihre Daten dann nicht mehr verarbeiten, es sei denn, es liegen zwingende schutzwürdige Gründe für die Verarbeitung vor.
- Recht auf Widerruf der Einwilligung (Artikel 7 Abs.3 DSGVO): Sofern wir Ihre personenbezogenen Daten auf Grundlage Ihrer Einwilligung verarbeiten, können Sie diese Einwilligung jederzeit widerrufen. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf bleibt hiervon unberührt.
- Recht auf Beschwerde bei einer Aufsichtsbehörde (Artikel 77 DSGVO): Sie haben das Recht, bei einer Datenschutz-Aufsichtsbehörde Beschwerde einzulegen, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten gegen datenschutzrechtliche Bestimmungen verstößt. Sie können Ihre Beschwerde insbesondere bei der zuständigen Datenschutzaufsichtsbehörde Ihres Aufenthaltsorts, Ihres Arbeitsplatzes, dem Sitz des Verantwortlichen oder dem Ort des mutmaßlichen Verstoßes einlegen. Die am Sitz des Verantwortlichen zuständige Aufsichtsbehörde ist:

  Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
  Ludwig-Erhard-Str. 22
  20459 Hamburg

Sie können Ihre Betroffenenrechte jederzeit durch Mitteilung uns gegenüber unter den im Abschnitt „Angaben zum Verantwortlichen“ dieser Datenschutzerklärung genannten Kontaktdaten schriftlich oder elektronisch geltend machen. Wir behalten uns in diesem Zusammenhang das Recht vor, Ihre Identität durch ein hierfür geeignetes Verfahren sicherzustellen.

Herunterladen der App (App and Play Store)

Sofern Sie unsere Applikation verwenden möchten, müssen Sie diese zunächst im App-Store Ihres Endgerätes herunterladen. Die Applikation wird derzeit im Apple App Store und im Google Play Store zum Download angeboten. Beim Download der Applikation werden bestimmte personenbezogene Daten an den jeweiligen App Store übermittelt.

Verarbeitete Daten:

- Nutzername des Store-Accounts
- E-Mail-Adresse
- Inhalt der Anforderung
- Betriebssystem des Endgerätes

Zwecke der Verarbeitung:

Die vorgenannten Daten werden vom Betreiber des jeweiligen App Stores benötigt, um Ihnen die Applikation zum Download zur Verfügung stellen zu können. Dabei erfolgt die Verarbeitung dieser Daten ausschließlich durch den Betreiber des jeweiligen App Stores und liegt daher außerhalb unseres Machtbereichs als Verantwortlicher.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr.9 DSGVO ist der Betreiber des App-Store (Apple Inc., 1 Apple Park Way, Cupertino, CA 95014, United States) und PlayStore (Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043, United States) über den Sie die Applikation downloaden. Bitte berücksichtigen Sie im Zusammenhang mit der Rechtsgrundlage für die Verarbeitung Ihrer Daten sowie im Hinblick auf die Speicherdauer die jeweils im Store hinterlegten Bestimmungen zum Datenschutz.

Informationen zum Datenschutz im Zusammenhang mit dem Google Play Store finden Sie unter Privacy Policy – Privacy & Terms – Google .

Informationen zum Datenschutz im Zusammenhang mit dem Apple App Store finden Sie unter Apple Legal - Legal - Privacy Policy - Apple .

Registrierung eines Kontos (T-Systems)

Zur Nutzung des mit der Applikation verbundenen Leistungsangebotes ist zunächst die Registrierung eines nutzerspezifischen Accounts (Nutzerkonto) erforderlich. Hierfür ist es erforderlich, dass Sie den Registrierungsprozess im Rahmen der Applikation durchlaufen und in diesem Zusammenhang bestimmte (personenbezogene) Daten bereitstellen.

Verarbeitete Daten:

- E-Mail-Adresse
- Passwort
- Geräte-Passkey (WebAuthn)
- Krankenversicherungsnummer (KVNR)

Zwecke der Verarbeitung:

Anlage und Absicherung des Nutzerkontos; eindeutige Zuordnung der Verordnung zur Versicherten-ID; Zwei-Faktor-Authentisierung über Passkey.

Rechtmäßigkeit der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Ihre ausdrückliche Einwilligung (vgl. Art. 6 Abs.1 lit.a und Art. 9 Abs.2 lit.a DSGVO). Ihre Einwilligung erteilen Sie dadurch, dass Sie im Rahmen des Registrierungsprozesses einen Haken in der hierfür vorgesehenen Checkbox setzen.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO und Art. 4 Nr. 15 DSGVO ist der Hosting-Provider des Backends der Applikation, T-Systems (T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main). T-Systems wird in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr.8 DSGVO für uns tätig und wurde entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages (AV-Vertrag) zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer personenbezogenen Daten dienen, verpflichtet.

Speicherdauer:

Bis zur Löschung des Nutzerkontos bzw. Widerruf Ihrer Einwilligung (unverändert zu den übrigen Registrierungsdaten). Nach Ablauf der Verordnung (90-120 Tage) wird Ihr Nutzerkonto automatisch gelöscht.

Risiken:

T-Systems ist als externer Dienstleister für den Betrieb zentraler technischer Komponenten unserer App verantwortlich. Aufgrund der Verarbeitung sensibler

personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) sowie der zentralen Systemverantwortung besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Verfügbarkeit der Anwendung sowie die Integrität und Vertraulichkeit der Nutzendendaten beeinträchtigen.

Hinweis zu Ihren Betroffenenrechten:
Sie können Ihre einmal erteilte Einwilligung gemäß Art. 7 Abs.3 DSGVO jederzeit mit Wirkung für die Zukunft gegenüber dem Verantwortlichen widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Zugriffsdaten und Hosting (T-Systems, Sentry)

Sobald Sie unsere Applikation aufrufen, übermittelt das dabei von Ihnen verwendete Endgerät automatisch Zugriffsdaten (sog. Log-Files) an den Hosting-Provider des Backends der Applikation. Beim Backend handelt es sich um den administrativen Bereich der Applikation, in welchem vor allem die Inhalte der Applikation verwaltet werden. Diese Log-Files enthalten unter anderem personenbeziehbare Daten.

Verarbeitete Daten:

- Nutzerinnen-ID
- IP-Adresse
- Datum und Uhrzeit der Anforderung
- Zeitzone
- Inhalt der Anforderung
- Zugriffsstatus/http-Statuscode
- Übertragene Datenmenge
- Inhalt, von welcher die Anforderung kommt (Referrer-URL)
- Betriebssystem des Endgerätes
- Version der App

Zwecke der Verarbeitung:

Die Log-Files werden zwingend benötigt, um die technische Funktionsfähigkeit der Applikation sicherzustellen. Insbesondere die Übermittlung Ihrer IP-Adresse ist

notwendig, um die Anzeige der Applikation auf dem von Ihnen verwendeten Endgerät zu ermöglichen. Die im Rahmen der Log-Files gespeicherten Daten werden von uns weder mit anderen Datenquellen zusammengeführt noch zur Identifikation einzelner Nutzer verwendet.

Rechtmäßigkeit der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe f) DSGVO. Das hierfür erforderliche „berechtigte Interesse“ folgt aus dem Wunsch, Ihnen ein sicheres und störungsfreies Nutzungserlebnis der Applikation zu bieten.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO sindder Hosting-Provider des Backends der Applikation, T-Systems (T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main) und der Anbieter des Dienstes Sentry (Functional Software Inc. , 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA . Alle vorgenannten Dienstleister werden in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO für den Verantwortlichen tätig und wurden auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:

Die Log-Files werden spätestens nach Ablauf von 90 Tagen automatisch gelöscht.

Risiken:

T-Systems ist als externer Dienstleister für den Betrieb zentraler technischer Komponenten unserer App verantwortlich. Aufgrund der Verarbeitung sensibler personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) sowie der zentralen Systemverantwortung besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Verfügbarkeit der Anwendung sowie die Integrität und Vertraulichkeit der Nutzendendaten beeinträchtigen.

Sentry ist als externer Dienstleister zur Fehlerüberwachung und Analyse von Systemereignissen in die Frieda-App eingebunden. Dabei erfolgt eine begrenzte Verarbeitung pseudonymisierter Nutzungsdaten. Aufgrund des potenziellen Bezugs zu personenbezogenen Informationen besteht ein moderates Schutzbedürfnis. Eine fehlerhafte Konfiguration oder unzulässige Datenverarbeitung könnte die Datensicherheit und das Vertrauen in die Anwendung beeinträchtigen.

Symptomerfassung und Kursnutzung (T-System)

Um eine individuelle Anpassung und Personalisierung der Kursinhalte zu ermöglichen haben Sie die Möglichkeit, vergangene und aktuelle Regelblutungsdaten, den Schweregrad einzelner Wechseljahresbeschwerden sowie tägliche Symptom-Einträge, Freitextnotizen und gesundheitsrelevante Kursangaben zu erfassen.

Verarbeitete Daten:

- Vergangene und aktuelle Regelblutung (Zykluslänge, Datum der letzten Periode)
- Schweregrad einzelner Wechseljahresbeschwerden (z. B. Hitzewallungen, Schlafqualität, Stimmung)
- Tägliche Symptom-Einträge, Freitextnotizen und gesundheitsrelevante Kursangaben der Nutzerin

Zwecke der Verarbeitung:
Die Verarbeitung der vorgenannten Daten dient der individuellen Personalisierung der Kursinhalte, der kontinuierlichen Optimierung von Übungen und Empfehlungen sowie der systematischen Evaluation des Behandlungserfolges.

Rechtmäßigkeit der Verarbeitung:
Die Rechtmäßigkeit der Datenverarbeitung stützen wir auf Art. 6 Abs. 1 lit. a i.V.m. Art. 9 Abs.2 Buchstabe a) DSGVO. Da auch Gesundheitsdaten als besondere Kategorien bezogener Daten verarbeitet werden, ist Ihre ausdrückliche Einwilligung in die Verarbeitung dieser Daten erforderlich. Ihre ausdrückliche Einwilligung erteilen Sie im Rahmen des Registrierungsprozesses durch das Setzen eines Hakens in der hierfür vorgesehenen Checkbox.

Empfänger der Daten:
Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO und Art. 4 Nr. 15 DSGVO ist der Hosting-Provider des Backends der Applikation, T-Systems (T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main). T-Systems wird in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr.8 DSGVO für uns tätig und wurde entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages (AV-Vertrag) zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer personenbezogenen Daten dienen, verpflichtet.

Speicherdauer:
Die Speicherung personenbezogener Daten erfolgt für die Dauer des ärztlich verordneten Nutzungszeitraums der DiGA (in der Regel 90 bis 120 Tage). Nach Ablauf dieses Zeitraums werden die betreffenden Daten unverzüglich gelöscht oder, sofern eine weitere Verarbeitung zu statistischen oder wissenschaftlichen Zwecken erfolgt, datenschutzkonform anonymisiert.

Risiken:

T-Systems ist als externer Dienstleister für den Betrieb zentraler technischer Komponenten unserer App verantwortlich. Aufgrund der Verarbeitung sensibler personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) sowie der zentralen Systemverantwortung besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Verfügbarkeit der Anwendung sowie die Integrität und Vertraulichkeit der Nutzendendaten beeinträchtigen.

Sicherheitsbenachrichtigung bei Anmeldungen von unbekannten Geräten (T-Systems)

Um potenziell unbefugte Zugriffe auf Ihr Nutzerkonto in Echtzeit zu erkennen und Sie unverzüglich darüber zu informieren, werden bei Anmeldungen von bislang unbekannten Geräten personenbezogene Daten verarbeitet. Dies ermöglicht es Ihnen, unmittelbar Maßnahmen zur Sicherung ihres Kontos zu ergreifen.

Verarbeitete Daten:

- E-Mail-Adresse
- Zeitstempel
- Gerätetyp
- Betriebssystem
- IP-Adresse
- Hash des zuletzt bekannten Geräts

Zwecke der Verarbeitung:
Echtzeit-Warnung bei potenziell unbefugtem Zugriff; Möglichkeit für die Nutzerin, das Konto unmittelbar zu sichern.

Rechtmäßigkeit der Verarbeitung:
Die Verarbeitung stützen wir auf Art. 6 Abs. 1 lit. f DSGVO, da wir, als Verantwortlicher im

Sinne der DSGVO, ein berechtigtes Interesse an der Sicherheit Ihres Nutzerkontos und dem Schutz Ihrer personenbezogener Daten haben.

Empfänger der Daten:
Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO und Art. 4 Nr. 15 DSGVO ist der Hosting-Provider des Backends der Applikation, T-Systems (T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main). T-Systems wird in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr.8 DSGVO für uns tätig und wurde entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages (AV-Vertrag) zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer personenbezogenen Daten dienen, verpflichtet.

Speicherdauer:
Die Log-Daten werden mindestens 90 Tage gespeichert. Der Benachrichtigungsstatus wird für die Dauer des Abonnements (in der Regel 90 bis 120 Tage) vorgehalten und anschließend gelöscht.

Risiken:

T-Systems ist als externer Dienstleister für den Betrieb zentraler technischer Komponenten unserer App verantwortlich. Aufgrund der Verarbeitung sensibler personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) sowie der zentralen Systemverantwortung besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Verfügbarkeit der Anwendung sowie die Integrität und Vertraulichkeit der Nutzendendaten beeinträchtigen.

Nutzungsanalyse (matomo)

Wir setzen im Rahmen der Webseite den Dienst matomo ein. Dabei handelt es sich um einen Analysedienst der InnoCraft (InnoCraft, 7 Waterloo Quay PO625, 6140 Wellington, New Zealand). matomo ermöglicht uns die Erfassung von Bewegungen im Rahmen der Appin Form so genannter Heatmaps.

Verarbeitete Daten:
- Nutzerinnen-ID
- Dauer der Sitzung
- Intensität / Häufigkeit der Nutzung
- Fortschritt im Kurs

Die vorgenannten Daten werden in anonymisierter Form erhoben und können keiner spezifischen Person zugeordnet werden. Sofern im Rahmen der eingesetzten Heatmap personenbezogene Daten (z.B. innerhalb von Eingabefeldern) sichtbar sein sollten, werden diese durch matomo automatisch unkenntlich gemacht.

Zwecke der Verarbeitung:
Die Verarbeitung der vorgenannten Daten ist erforderlich, damit die App ausgewertet und besser an die Bedürfnisse der Nutzer angepasst werden kann.

Rechtmäßigkeit der Verarbeitung:
Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe a) DSGVO.

Empfänger der Daten:
Empfänger Ihrer anonymisierten Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Dienst matomo (InnoCraft, 7 Waterloo Quay PO625, 6140 Wellington, New Zealand). Der Anbieter von matomo wird in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurden von uns entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.
Bitte beachten Sie in diesem Zusammenhang, dass InnoCraft ihren Geschäftssitz in Neuseeland unterhält. Eine Datenübermittlung nach Neuseeland ist grundsätzlich nicht vorgesehen, kann jedoch auch nicht abschließend ausgeschlossen werden. Es gelten insoweit die Ausführungen vom Abschnitt „Datenübermittlung in Drittländer“.

Speicherdauer:
Da ausschließlich anonymisierte Nutzungsdaten verarbeitet werden, die keinen Personenbezug aufweisen, werden diese für einen unbegrenzten Zeitraum gespeichert.

Risiken:

Da ausschließlich anonymisierte Daten verarbeitet werden, besteht kein Personenbezug und daher kein spezifisches Schutzbedürfnis.

Empfang von werblichen Newslettern (Brevo)

Als Bestandteil unseres Leistungsangebotes bieten wir Ihnen die Möglichkeit zur Anmeldung für unseren Newsletter. Für die Erstellung, den Versand und die Auswertung unserer Newsletter ist es erforderlich, dass personenbezogene Daten von Ihnen verarbeitet werden.

Verarbeitete Daten:

- Vorname, Nachname
- E-Mail-Adresse
- Anonymisierte Nutzungsdaten (z.B. Öffnungs- und Klickrate)
- Anmelde- und Bestätigungszeitpunkt
- IP-Adresse
- Protokolldaten

Zwecke der Verarbeitung:

Die Verarbeitung der vorgenannten Daten ist erforderlich, damit wir Ihnen personalisierte Newsletter und Informationen zusenden und eine anonymisierte Auswertung des Erfolgs unserer Newsletter in Bezug auf die Klick- und Öffnungsrate messen können.

Rechtsgrundlage der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe a) DSGVO. Ihre Einwilligung zum Empfang unserer Newsletter und Informationen können Sie über unser Formular auf unserer Webseite erteilen.

Die Anmeldung zu unserem Newsletter erfolgt in einem sog. Double-Opt-In-Verfahren. D.h. Sie erhalten nach der Anmeldung eine E-Mail, in der Sie um die Bestätigung Ihrer Anmeldung gebeten werden. Diese Bestätigung ist notwendig, damit sich niemand mit einer fremden E-Mail-Adresse anmelden kann. Die Anmeldungen zum Newsletter werden protokolliert, um den Anmeldeprozess entsprechend den rechtlichen Anforderungen nachweisen zu können.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Anbieter des Dienstes Brevo (Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin). Der Anbieter von Brevo wird in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurden von uns entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:

Die in diesem Rahmen von uns verarbeiteten Daten werden von uns längstens bis zum Widerruf Ihrer Einwilligung im Empfang unserer Newsletter und Informationen gespeichert. Sie können Ihre einmal erteilte Einwilligung in den Empfang unserer Newsletter und Informationen jederzeit in der Fußzeile der Newsletter und Informationen, die Sie von uns empfangen oder auch per E-Mail an hello@frieda.health widerrufen.

Risiken:

Brevo wird für den Versand von Newslettern eingesetzt. Zwar werden im Rahmen dieser Verarbeitungen keine Gesundheitsdaten gemäß Art. 9 DSGVO verarbeitet, durch Inhalte oder Bezug zur App-Nutzung können jedoch indirekt Rückschlüsse auf gesundheitliche Themen möglich sein. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Kommunikation mit Nutzenden beeinträchtigen.

Kontaktverwaltung und E-Mailing (Brevo)

Wir setzen zur Verwaltung des Unternehmens inklusive Kontaktverwaltung und transaktionalen Emailing das Tool Brevo (Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin) ein. Brevo ermöglicht uns eine einfache und effiziente Unternehmensverwaltung und -organisation.

Verarbeitete Daten:

- E-Mail-Adresse

Zwecke der Verarbeitung:

Die Verarbeitung der vorgenannten Daten ermöglicht uns eine einfache und effiziente Unternehmensverwaltung und -organisation mit dem Ziel einer verbesserten Kundenbeziehung und einem verbesserten Kundenservice.

Rechtmäßigkeit der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe b) DSGVO. Insoweit dient die Kontaktverwaltung vor allem der Anbahnung und Abwicklung von Vertragsverhältnissen zwischen Ihnen und uns.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Anbieter des Dienstes Brevo (Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin). Der Anbieter von Brevo wird in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurden von uns entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:

Die verarbeiteten Daten werden von uns nur so lange gespeichert, wie dies für die Erreichung der mit dieser Verarbeitungstätigkeit verfolgten Zwecke erforderlich ist. Anschließend werden die Daten von uns gelöscht, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

Brevo wird für die Kontaktverwaltung sowie den Versand transaktionaler E-Mails eingesetzt. Zwar werden im Rahmen dieser Verarbeitungen keine Gesundheitsdaten gemäß Art. 9 DSGVO verarbeitet, durch Inhalte oder Bezug zur App-Nutzung können jedoch indirekt Rückschlüsse auf gesundheitliche Themen möglich sein. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Kommunikation mit Nutzenden und die Nutzung der Frieda-App beeinträchtigen.

Kundinnensupport (Zendesk)

Wir setzen zur Verwaltung des Unternehmens inklusive Kontaktverwaltung das Tool Zendesk (Zendesk EMEA HQ, 55 Charlemont Pl, Saint Kevin’s, Dublin, D02 F985, Irland) ein. Zendesk ermöglicht uns eine einfache und effiziente Unternehmensverwaltung und -organisation.

Verarbeitete Daten:

- E-Mail-Adresse
- Freiwillig mitgeteilte Inhalte (einschließlich ggf. Gesundheitsdaten)

Zwecke der Verarbeitung:

Die Verarbeitung der vorgenannten Daten ermöglicht uns eine einfache und effiziente Unternehmensverwaltung und -organisation mit dem Ziel einer verbesserten Kundenbeziehung und einem verbesserten Kundenservice.

Rechtmäßigkeit der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe b) DSGVO. Insoweit dient die Kontaktverwaltung vor allem der Anbahnung und Abwicklung von Vertragsverhältnissen zwischen Ihnen und uns.

Wenn Sie uns im Rahmen einer Supportanfrage freiwillig gesundheitsbezogene Angaben übermitteln (z. B. zu Beschwerden oder Diagnosen), verarbeiten wir diese ausschließlich auf Grundlage Ihrer ausdrücklichen Einwilligung, die Sie bei Erstellung Ihres Nutzerkontos durch Setzen einer entsprechenden Checkbox erteilen. Die Mitteilung solcher Daten ist freiwillig und für die Nutzung des Kundensupports nicht erforderlich.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Anbieter des Dienstes Zendesk (Zendesk EMEA HQ, 55 Charlemont Pl, Saint Kevin's, Dublin, D02 F985, Irland). Der Anbieter von Zendesk wird in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurden von uns entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:

Die verarbeiteten Daten werden von uns nur so lange gespeichert, wie dies für die Erreichung der mit dieser Verarbeitungstätigkeit verfolgten Zwecke erforderlich ist. Anschließend werden die Daten von uns gelöscht, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

Zendesk ist als externer Dienstleister für die Verwaltung von Kundinnenanfragen unserer App verantwortlich. Aufgrund der Verarbeitung sensibler personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Vertraulichkeit der Nutzendendaten beeinträchtigen.

Fehler- und Performance-Monitoring (Sentry)

Zur Gewährleistung der technischen Stabilität, Fehlererkennung und -behebung sowie zur Optimierung der Performance unserer App ist die Verarbeitung Ihrer personenbezogenen Daten notwendig. Die Erfassung erfolgt jedoch ausschließlich

pseudonymisiert und dient ausschließlich der Identifikation technischer Probleme ohne direkte Nutzerinnen-Identifikation.

Verarbeitete Daten:

- Pseudonymisierte Nutzerinnen-ID
- Zeitstempel
- Gekürzte IP-Adresse
- Geräte-/Betriebssysteminformationen
- Stack-Traces und Log-Nachrichten (können in Ausnahmefällen Freitext enthalten)

Zwecke der Verarbeitung:
Die Verarbeitung der vorgenannten Daten ermöglicht uns eine effektive und datenschutzbewusste Überwachung der technischen Stabilität und Leistung der App mit dem Ziel, Fehler frühzeitig zu erkennen, Störungen schnell zu beheben und somit ein zuverlässiges und sicheres Nutzungserlebnis sicherzustellen..

Rechtmäßigkeit der Verarbeitung:
Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs. 1 Buchstabe f) DSGVO. Das hierfür erforderliche „berechtigte Interesse“ stützen wir auf unseren Wunsch, Ihnen ein sicheres und störungsfreies Nutzungserlebnis unserer App zu bieten. Andernfalls wäre eine Nutzung unserer App für Sie nicht möglich..

Empfänger der Daten:
Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Anbieter des Dienstes Sentry (Functional Software Inc., 45 Fremont Street, San Francisco, USA)). Der Anbieter von Sentry wird in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurde von uns entsprechend auf Grundlage eines AV-Vertrags zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:
Die verarbeiteten Daten werden maximal 90 Tage gespeichert. Anschließend erfolgt eine automatische Löschung, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

Sentry ist als externer Dienstleister für den Betrieb zentraler technischer Komponenten unserer App verantwortlich. Aufgrund der zentralen Systemverantwortung besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall könnte die Verfügbarkeit der Anwendung beeinträchtigen.

Fehlererfassung und Bug-Management (Jira)

Zur internen Erfassung, Analyse und Behebung technischer Fehler („Bugs“) innerhalb unserer Frieda-App setzen wir ein Fehler- und Vorgangsmanagementsystem ein. Dieses dient der Qualitätssicherung, Stabilitätsüberwachung und kontinuierlichen Verbesserung der Anwendung.

Verarbeitete Daten:

- Zeitstempel
- App-Version
- Betriebssystem
- Log-Daten

Zwecke der Verarbeitung:

Die Verarbeitung der vorgenannten Daten ermöglicht uns die Erfassung und Behebung technischer Fehler innerhalb der Frieda-App um Ihnen die Funktionalität, Stabilität und Sicherheit unserer Anwendung gewährleisten zu können.

Rechtmäßigkeit der Verarbeitung:

Die Verarbeitung stützen wir auf Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in der Aufrechterhaltung und Verbesserung der technischen Funktionsfähigkeit und Sicherheit unserer Anwendung.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO ist der Anbieter des Dienstes Jira (Atlassian. Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australien), der im Rahmen der Fehlererfassung und -verwaltung eingesetzt wird. Der Anbieter wird in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO für uns tätig und ist auf Grundlage eines Auftragsverarbeitungsvertrages (AV-Vertrag) zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs) verpflichtet.

Speicherdauer:
Die verarbeiteten Daten werden nur so lange gespeichert, wie dies zur Fehleranalyse und -behebung erforderlich ist. Anschließend werden die Daten von uns gelöscht, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

Im Rahmen der Fehlererfassung kann in Einzelfällen ein Bezug zu personenbezogenen Daten nicht vollständig ausgeschlossen werden. Aufgrund der technischen Natur der Datenverarbeitung besteht ein moderates Schutzbedürfnis. Ein Ausfall oder eine

fehlerhafte Verarbeitung könnte die Behebung technischer Fehler und die Stabilität der Anwendung beeinträchtigen.

Funktionen-Management (LaunchDarkly)

Um neue Funktionen kontrolliert und risikominimiert bereitzustellen, werden im Rahmen unseres Feature-Flag-Managements bestimmte pseudonymisierte und technische Informationen verarbeitet. Dies ermöglicht eine gezielte Steuerung von Rollouts, A/B-Tests sowie eine schrittweise Freischaltung von Funktionalitäten – insbesondere zur Reduktion potenzieller Fehlfunktionen im Live-Betrieb. Die Verarbeitung erfolgt dabei ausschließlich pseudonymisiert.

Verarbeitete Daten:

- Pseudonymisierte Nutzerinnen-ID
- Metadaten zu aktivierten Feature-Flags (Key, Variation, Zeitstempel)
- Client- & Umfeldinformationen (App-Version, OS-Typ)

Zwecke der Verarbeitung:
Die Verarbeitung der vorgenannten Daten ermöglicht uns eine gezielte, flexible und risikominimierte Steuerung von Funktionsfreigaben innerhalb der App mit dem Ziel, neue Funktionen sicher, datenschutzkonform und bedarfsgerecht auszurollen.

Rechtmäßigkeit der Verarbeitung:
Die Rechtmäßigkeit der Verarbeitung stützen wir auf Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in der sicheren, stabilen und kontrollierten Auslieferung neuer Funktionen, der risikominimierten Durchführung technischer Rollouts sowie der fortlaufenden Optimierung der App-Leistung.

Empfänger der Daten:
Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr.9 DSGVO ist der Anbieter des Dienstes LaunchDarkly (Catamorphic Co. dba LaunchDarkly, Oakland USA. LaunchDarkly wird in diesem Zusammenhang als Auftragsverarbeiter im Sinne von Art. 4 Nr.8 DSGVO für uns tätig und wurde von uns entsprechend auf Grundlage eines AV-Vertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer personenbezogenen Daten dienen, verpflichtet.

Speicherdauer:
Die verarbeiteten Daten werden nur so lange gespeichert, wie dies zur Erreichung der vorgenannten Zwecke erforderlich ist. Eine automatische Löschung erfolgt je nach Aktivität der Nutzerin innerhalb von 30 bis 150 Tagen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

LaunchDarkly wird für die zentrale Steuerung und kontrollierte Freigabe von App-Funktionalitäten eingesetzt. Aufgrund der technischen Schlüsselrolle im Rahmen des Feature-Flag-Managements besteht ein erhöhtes Schutzbedürfnis hinsichtlich der Verfügbarkeit und Integrität der Anwendung. Ein Ausfall oder eine fehlerhafte Verarbeitung kann zu Fehlfunktionen, eingeschränkter Nutzererfahrung oder temporären Ausfällen einzelner App-Komponenten führen.

Weitergabe von Daten an Dritte

Wir und die von uns eingesetzten Auftragsverarbeiter werden Ihre Daten grundsätzlich nur dann an Dritte im Sinne von Art. 4 Nr. 10 DSGVO weitergeben, wenn

- Sie zur Weitergabe gemäß Art. 6 Abs. 1 Buchstabe a) DSGVO Ihre ausdrückliche Einwilligung gegeben haben;
- die Weitergabe gemäß Art. 6 Abs. 1 Buchstabe b) DSGVO für die Anbahnung oder die Abwicklung eines Vertragsverhältnisses mit Ihnen und uns erforderlich ist;
- wir zur Weitergabe gemäß Art. 6 Abs. 1 Buchstabe c) DSGVO gesetzlich verpflichtet sind, oder
- die Weitergabe gemäß Art. 6 Abs. 1 Buchstabe f) DSGVO auf Grundlage unseres berechtigten Interesses zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen erforderlich ist und kein Grund zu der Annahme besteht, dass Sie ein überwiegendes, schutzwürdiges Interesse an der Nichtweitergabe Ihrer Daten haben.

Kontaktaufnahme mit dem Verantwortlichen

Sie haben jederzeit die Möglichkeit, unter anderem im Rahmen der App, mit uns in Verbindung zu treten und Anfragen zu stellen. Die Bearbeitung Ihrer Anfrage(n) macht

es erforderlich, dass wir Kenntnis von Ihren personenbezogenen Daten nehmen, die Sie im Rahmen Ihrer Anfrage an uns übermitteln.

Verarbeitete Daten:

- Vorname, Nachname
- E-Mail-Adresse
- Datum und Uhrzeit der Anfrage
- Inhalt der Anfrage

Zwecke der Verarbeitung:

Die Verarbeitung der von Ihnen im Rahmen der Kontaktaufnahme mit uns übermittelten Daten erfolgt von unserer Seite ausschließlich zum Zweck der Erfassung, Bearbeitung und Beantwortung Ihrer Anfrage. Bitte beachten Sie, dass produktbezogene Beschwerden als Teil der Marktbeobachtung von uns herangezogen werden können, um die Qualität und Sicherheit der angebotenen Leistungen zu bewerten (Feedback-Management).

Rechtsgrundlage der Verarbeitung:

Die Rechtmäßigkeit dieser Datenverarbeitung stützen wir auf Art. 6 Abs.1 Buchstabe a) DSGVO. Ihre Einwilligung erteilen Sie dadurch, dass Sie Ihre Nachricht (z.B. per E-Mail) aktiv an uns übermitteln.

Empfänger der Daten:

Empfänger Ihrer personenbezogenen Daten im Sinne von Art. 4 Nr. 9 DSGVO sind die Provider der E-Mail-Software, die von uns für den Empfang sowie die Bearbeitung von E-Mails verwendet wird. Hierbei handelt es sich um GoogleMail (Google Ireland Ltd., Google Building, Gordon House, 4 Barrow St., Grand Canal Dock, Dublin 4, D04 V4X7, Irland) und Zendesk (Zendesk EMEA HQ, 55 Charlemont PI, Saint Kevin’s, Dublin, D02 F985, Irland).

Darüber hinaus verwenden wir für die Verwaltung Ihrer Anfragen das Customer-Relationship-Management-Tool (CRM-Tools) Brevo (Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin).

Für die Organisation und Verwaltung setzen wir außerdem das Projektmanagement-Tool Jira (Atlassian. Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australien).

Bitte beachten Sie, dass hinter Google ein US-amerikanischer Mutterkonzern steht. Darüber hinaus unterhält Atlassian seinen Geschäftssitz in Australien. Insoweit weisen wir Sie vorsorglich darauf hin, dass Sie mit Ihrer Zustimmung zu dieser Datenschutzerklärung auch einer potenziellen Übermittlung Ihrer personenbezogenen

Daten in Drittstaaten (vordringlich USA) zustimmen, da wir eine solche Datenübermittlung nicht abschließend ausschließen können.

Die Anbieter unserer E-Mail-Software und der eingesetzten Tools werden in diesem Zusammenhang als Auftragsverarbeiter für uns tätig und wurden entsprechend auf Grundlage eines Auftragsverarbeitungsvertrages zur Einrichtung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs), die dem Schutz Ihrer Daten dienen, verpflichtet.

Speicherdauer:

Die verarbeiteten Daten werden von uns nur solange gespeichert, wie dies für die Bearbeitung und Beantwortung Ihrer Anfrage erforderlich ist. Anschließend werden die Daten von uns gelöscht, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Risiken:

Brevo wird für den Versand von Newslettern, die Kontaktverwaltung sowie den Versand transaktionaler E-Mails eingesetzt. Zwar werden im Rahmen dieser Verarbeitungen keine Gesundheitsdaten gemäß Art. 9 DSGVO verarbeitet, durch Inhalte oder Bezug zur App-Nutzung können jedoch indirekt Rückschlüsse auf gesundheitliche Themen möglich sein. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Kommunikation mit Nutzenden und die Nutzung der Frieda-App beeinträchtigen.

Zendesk ist als externer Dienstleister für die Verwaltung von Kundinnenanfragen unserer App verantwortlich. Aufgrund der Verarbeitung sensibler personenbezogener Daten (einschließlich Gesundheitsdaten gemäß Art. 9 DSGVO) besteht ein erhöhtes Schutzbedürfnis. Ein Ausfall oder eine fehlerhafte Verarbeitung könnte die Vertraulichkeit der Nutzendendaten beeinträchtigen.

Jira wird zur internen Bearbeitung von Supportanfragen und Entwicklungstickets eingesetzt. Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO erfolgt nur in Ausnahmefällen, wenn Nutzende derartige Informationen freiwillig übermitteln; eine Verpflichtung hierzu besteht nicht. Aufgrund des Anbietersitzes in Australien und möglicher Datenübermittlungen in Drittstaaten besteht das potenzielle Risiko staatlicher Zugriffe. Ein Ausfall kann die Bearbeitung nutzerbezogener Anliegen sowie die Weiterentwicklung der App erheblich beeinträchtigen.

GoogleMail wird zur Bearbeitung eingehender Nutzeranfragen genutzt. Aufgrund des US-amerikanischen Mutterkonzerns kann ein Zugriff durch US-Behörden nicht gänzlich ausgeschlossen werden. Bei sensiblen Inhalten, etwa mit Gesundheitsbezug, besteht ein erhöhtes Risiko für den Verlust der Vertraulichkeit. Ein Ausfall kann zu Verzögerungen oder Ausfällen in der Nutzerkommunikation führen.

Einbindung von Inhalten Dritter

Unter Umständen werden im Rahmen der App auch Inhalte Dritter, wie Videos oder Grafiken eingebunden. Die Einbindung dieser Inhalte setzt voraus, dass die Anbieter dieser (Drittanbieter) Ihre IP-Adresse wahrnehmen, da die Inhalte ansonsten nicht im Rahmen der App angezeigt werden können.
Wir sind bemüht, nur Inhalte von Drittanbietern zu nutzen, die Ihre IP-Adresse ausschließlich zum Zweck der Auslieferung der Inhalte verwenden. Wir haben jedoch keinen Einfluss darauf, falls Drittanbieter Ihre IP-Adresse für weitere Zwecke, wie z.B. statistische Auswertungen, verarbeiten. Soweit uns ein solches Vorgehen bekannt wird, werden Sie im Rahmen dieser Datenschutzerklärung informiert.

Einbindung von Software-Komponenten

Eine Software Bill of Materials (SBOM), auf Deutsch auch Software-Stückliste genannt, ist eine detaillierte Auflistung aller Komponenten und Abhängigkeiten einer Software. Sie ist eine ganzheitliche Bestandsaufnahme, die alle Module, Bibliotheken, Tools und andere Bestandteile einer Softwareanwendung beschreibt. Die Software-Stückliste kann jederzeit in den Einstellungen der Frieda-App eingesehen werden.

Unsere Dienstleister und Auftragsverarbeiter

Im Rahmen der Bereitstellung und Nutzung unsere Frieda-App werden personenbezogene Daten durch sorgfältig ausgewählte Auftragsverarbeiter im Sinne von Artikel 28 DSGVO verarbeitet. Diese Dienstleister wurden von uns als Verantwortlichen vertraglich zur Einhaltung der datenschutzrechtlichen Vorgaben sowie zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen (TOMs) verpflichtet.

Nachfolgend sind alle derzeit eingesetzten Auftragsverarbeiter aufgeführt:

Nr	Auftragsverarbeiter	Adresse	Zweck
1	T-Systems International GmbH	Hahnstraße 43d, 60528 Frankfurt am Main, Deutschland	Hosting / Backend-Betrieb / Konto- und Kursverwaltung
2	Functional Software Inc. (Sentry)	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fehler- und Performance-Monitoring
3	InnoCraft Ltd. (matomo)	7 Waterloo Quay PO625, 6140 Wellington, Neuseeland	Nutzungsanalyse / Heatmaps
4	Sendinblue GmbH (Brevo)	Köpenicker Straße 126, 10179 Berlin, Deutschland	Newsletter-Versand / Kontaktverwaltung / transaktionale E-Mails
5	Zendesk EMEA HQ	55 Charlemont Place, Saint Kevin's, Dublin D02 F985, Irland	Kundinnensupport
6	Catamorphic Inc. (LaunchDarkly)	1999 Harrison St., Suite 1100, Oakland, CA 94612, USA	Feature-Flag- und Funktions-management
7	Google Ireland Ltd. (Google Mail)	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland	Kommunikation / E-Mail-Hosting
8	Atlassian Pty Ltd (Jira)	Level 6, 341 George Street, Sydney NSW 2000, Australien	Bearbeitung und Nachverfolgung technischer Fehler (Bugs) sowie Projekt- und Ticketmanagement

Im Rahmen der Verordnung (EU) 2017/745 über Medizinprodukte (MDR) sowie der Vorgaben für digitale Gesundheitsanwendungen (DiGA) des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) stellt die Frieda Health GmbH ergänzende Angaben zu den in dieser Datenschutzerklärung benannten Dienstleistern bereit. Hierzu

zählen sowohl Auftragsverarbeiter im Sinne des Art. 28 DSGVO als auch sonstige Dienstleister, die eigenständig Leistungen erbringen (z. B. App- und Store-Anbieter).

Die Angaben umfassen insbesondere den Namen des Mutterkonzerns, den Standort der Datenverarbeitung durch den Mutterkonzern sowie die Zuordnung des Standorts zu einer der folgenden Kategorien: Inland, EU-Mitgliedstaat, Vertragsstaat des Europäischen Wirtschaftsraums (EWR), Schweiz oder Drittstaat.

Für Dienstleister mit Sitz in einem Drittstaat wird gemäß Art. 45 DSGVO angegeben, ob ein Angemessenheitsbeschluss der Europäischen Kommission besteht. Liegt kein solcher Beschluss vor, erfolgt eine Übermittlung nur, soweit erforderlich, auf Grundlage geeigneter Garantien nach Art. 46 DSGVO (z. B. Standardvertragsklauseln) und unter Anwendung zusätzlicher Schutzmaßnahmen.

Datenübermittlungen an Dienstleister erfolgen ausschließlich, soweit dies zur Bereitstellung unserer Leistungen erforderlich ist oder eine entsprechende Rechtsgrundlage besteht.

Die nachfolgende Übersicht enthält die entsprechenden Informationen zu den von der Frieda Health GmbH eingesetzten Dienstleistern (einschließlich Auftragsverarbeitern):

Dienstleister	Anbieter	Mutterkonzern	Standort der Datenverarbeitung (Mutterkonzern)	Zuordnung	Angemessenheitsbeschluss gemäß Art. 45 DSGVO
T-Systems	T-Systems International GmbH, Frankfurt a. M.	Deutsche Telekom AG	Deutschland	Inland	–
Sentry	Functional Software Inc., San	Functional Software Inc.	USA	Drittstaat	EU-US Data Privacy Framework (DPF)

	Francisco (USA)				
matomo	InnoCraft Ltd., Wellington (NZ)	InnoCraft Ltd.	Neuseeland	Drittstaat	Angemessenheitsbeschluss für Neuseeland
Brevo / Sendinblue	Sendinblue GmbH, Berlin	Sendinblue SAS	Frankreich	EU-Mitgliedstaat	–
Zendesk	Zendesk EMEA HQ, Dublin (IRL)	Zendesk Inc.	USA	Drittstaat	EU-US Data Privacy Framework (DPF)
LaunchDarkly	Catamorphic Inc. d/b/a LaunchDarkly, Oakland (USA)	Catamorphic Inc.	USA	Drittstaat	EU-US Data Privacy Framework (DPF)
Google Mail	Google Ireland Ltd., Dublin (IRL)	Google LLC / Alphabet Inc.	USA	Drittstaat	EU-US Data Privacy Framework (DPF)
Jira	Atlassian Pty Ltd, Sydney (AUS)	Atlassian Corp Plc (US)	USA	Drittstaat	EU-US Data Privacy Framework (DPF)
Apple App Store	Apple Inc., Cupertino (USA)	Apple Inc.	USA	Drittstaat	Teilweise DPF-zertifiziert

Google Play Store	Google LLC, Mountain View (USA)	Google LLC / Alphabet Inc.	USA	Drittstaat	EU-US Data Privacy Framework (DPF)

Löschkonzept und Datenaufbewahrung

Die Frieda Health GmbH hat ein Löschkonzept gemäß den Vorgaben BfArM, der MDR sowie der DSGVO implementiert. Es gewährleistet die Einhaltung der Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 DSGVO, insbesondere Zweckbindung, Datenminimierung und Speicherbegrenzung.

Personenbezogene Daten werden nur so lange gespeichert, wie dies zur Erfüllung des jeweiligen Verarbeitungszwecks erforderlich ist. Nach Wegfall des Verarbeitungszwecks erfolgt die Löschung oder eine datenschutzkonforme Anonymisierung, sofern hier keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

Im Rahmen der Nutzung der Frieda-App werden sämtliche personenbezogenen und gesundheitsbezogenen Daten nach Ablauf des ärztlich verordneten Nutzungszeitraums (in der Regel 90 bis 120 Tage) automatisiert gelöscht. Das Nutzerkonto wird deaktiviert und anschließend vollständig entfernt.

Die Löschung erfolgt auf Grundlage festgelegter technischer und organisatorischer Maßnahmen (TOMs) nach Art. 32 DSGVO. Unsere Auftragsverarbeiter sind vertraglich verpflichtet, Daten nach denselben Maßstäben zu löschen.

Die Wirksamkeit und Vollständigkeit unserer Löschprozesse wird regelmäßig überprüft und dokumentiert.

Aktualisierung dieser Datenschutzerklärung

Wir behalten uns das Recht vor, diese Datenschutzerklärung mit Wirkung für die Zukunft zu aktualisieren, um auf Gesetzesänderungen, Änderungen der Rechtsprechung oder Veränderungen der wirtschaftlichen Verhältnisse angemessen reagieren zu können. Eine

von uns beabsichtigte Änderung dieser Datenschutzerklärung werden wir Ihnen gegenüber rechtzeitig mitteilen. Ihre Rechte als betroffene Person im Sinne der DSGVO werden niemals durch eine Änderung dieser Datenschutzerklärung eingeschränkt.