Topfit.App

Konzept zum Datenschutz

Die **Topfit.App** ist eine Online-Plattform im Bereich des betrieblichen Gesundheitsmanagements, welche Arbeitgeber und Krankenkassen ihren Mitarbeitern und Versicherten zur Verfügung stellen können. Die Topfit GmbH entwickelt und betreut die **Topfit.App** ausschließlich in-house ohne weitere Subunternehmer (ausgenommen Hosting, siehe Punkt 1).

1 Data-Hosting

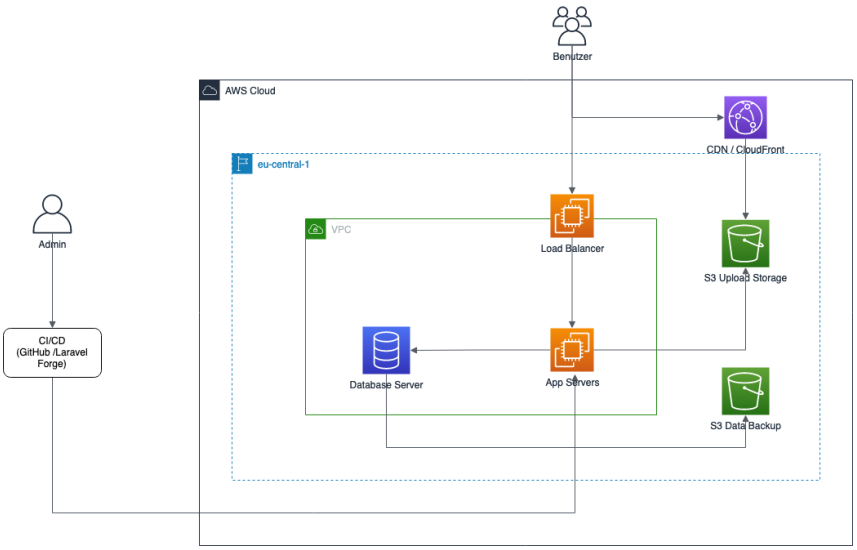
Die **Topfit.App** wird ausschließlich auf Amazon Web Services (AWS) gehostet. Die Server stehen physikalisch bei AWS in Frankfurt a.M., die komplette Datenverarbeitung findet also innerhalb der **Bundesrepublik Deutschland** statt.

Topfit nimmt dabei den VPC-Service in Anspruch. VPC steht für »Virtual Private Cloud« und stellt einen logisch isolierten Abschnitt der AWS-Cloud dar. Eine Datenübertragung in andere AWS-Regionen außerhalb der EU findet nicht statt. Die Software läuft in einem getrennten und ausschließlich für die **Topfit.App** verwendeten AWS-Konto. Zugriff hierauf haben ausschließlich Mitarbeiter der Topfit GmbH, die direkt an diesem Projekt arbeiten. Die Datenbanken sind von außen nicht zugänglich, nur durch die Anwendungsserver innerhalb der VPC selbst.

Anschrift:
Amazon Web Services EMEA SRL
38 Avenue John F. Kennedy
L-1855 Luxembourg

Amazon Web Services ist umfassend zertifiziert, bspw. nach ISO 27001, 27017 und 27018. Ferner ist AWS konform mit dem CISPE-Verhaltenskodex (CISPE Code of Conduct) für den Datenschutz.

Weitere Informationen dazu finden sich hier:
https://aws.amazon.com/de/compliance/data-privacy/



2 Datenschutz

2.1 Erhebung von personenbezogenen Daten

Personenbezogene Daten werden ausschließlich von der Topfit GmbH erhoben und verarbeitet. Es wird sichergestellt, dass diese Daten zu keinen anderen Zwecken als den vertraglich festgelegten verarbeitet werden. (Siehe hierzu bitte unter “5. Arten personenbezogener Daten”.)

2.2 Einsatz von Verschlüsselung in Aufbewahrung und Transport

Die Erhebung von personenbezogenen Daten über die **Topfit.App** findet ausschließlich verschlüsselt (TLS, Stand der Technik) statt. Die Daten werden bei AWS stets verschlüsselt aufbewahrt. Das heißt, die Daten sind sowohl im Transit (überall außerhalb der VPC) als auch »at Rest« (Festplatte des Datenbank-Servers) verschlüsselt.

2.3 Angaben zu den Datenschutzbestimmungen

Sind die Datenschutzbestimmungen bei erstmaliger Web-App/Webseiten- Nutzung sofort einsehbar (z. B. Pop-Up Info-Frame)?

Ja, per Link „Datenschutz“ im Footer-Bereich der Startseite bzw. im Footer-Bereich der Registrierungs- oder Loginmaske (https://topfit.app/info/privacy-policy).

Sind die Datenschutzbestimmungen innerhalb der Web-App/Webseite leicht auffindbar und einsehbar?

Ja, auf jeder Seite innerhalb des Footer-Bereiches oder innerhalb der ersten Navigationsebene.

Wird in den Datenschutzbestimmungen die Erhebung, Verarbeitung und Nutzen personenbezogener Daten beschrieben?

Ja

Liegt ein den Anforderungen von § 5 TMG („leicht erkennbar“, „unmittelbar erreichbar“, „ständig verfügbar“; zudem ggf. § 55 Abs. 2 RStV-Anforderung) entsprechendes Impressum vor?

Ja, im Footer-Bereich der Webseite oder innerhalb der ersten Navigationsebene.

2.4 Arten von personenbezogenen Daten

2.4.1 Welche Nutzungsdaten (vgl. § 15 Abs. 1 TMG) werden von der Web-Applikation automatisch verarbeitet?

Bei der erstmaligen Registrierung eines Benutzers werden folgende Daten erhoben:

Attribut	**Klarname**	**Zweck der Datenverarbeitung**	**Attributtyp**
id	Identifikator	Einmalige, eindeutige Benutzerkennung	Automatisch generiert
username	Benutzername	Einmalige, eindeutige Benutzerkennung	Automatisch generiert Ergibt sich aus dem angegeben Webcode
salutation	Anrede	Personalisierte Ansprache des Benutzers	Optionales Feld
firstname	Vorname	Personalisierte Ansprache des Benutzers Anzeige bei Kommentaren Anzeige bei Reaktionen Anzeige in Posts	Optionales Feld
lastname	Zuname	Personalisierte Ansprache des Benutzers Anzeige bei Kommentaren Anzeige bei Reaktionen Anzeige in Posts	Optionales Feld

Attribut	Klarname	Zweck der Datenverarbeitung	Attributtyp
user_type	Benutzertyp	Autorisierung des Benutzers	Automatisch generiert Ergibt sich aus dem angegeben Webcode
email	E-Mail-Adresse	Nachweis der Authentizität des Benutzers Verifizierung des Benutzers Anfordern eines neuen Passworts Kommunikation von Terminvergaben	Pflichtfeld
email_verified_at	E-Mail-Adresse verifiziert am	Verifizierung des Benutzers	Automatisch generiert, nachdem der Benutzer die Verifizierungsseite geöffnet hat
password	Kennwort	Authentifizierung des Benutzers	Pflichtfeld Das Benutzerkennwort durchläuft eine Hashfunktion (Bcrypt)
remember_token		Sicherheitsmaßnahme um „Remember Me“ Cookie Hijacking zu verhindern.	Automatisch generiert
last_seen	Zuletzt in der Web-Applikation angemeldet	Onlineindikator von Benutzern	Automatisch generiert
client_id	Mandant	Zuweisung des Benutzers zum Mandanten Zuordnung der App-Inhalte Zuordnung von Benutzern erstellten Inhalten	Automatisch generiert Ergibt sich aus dem angegeben Webcode

Attribut	Klarname	Zweck der Datenverarbeitung	Attributtyp
business_unit_id	Strategische Geschäftseinheit	Zuweisung des Benutzers zu einer Strategischen Geschäftseinheit Zuordnung der App-Inhalte Zuordnung von Benutzern erstellten Inhalten	Pflichtfeld
region_id	Region	Zuweisung des Benutzers zu einer Region Zuordnung der App-Inhalte Zuordnung von Benutzern erstellten Inhalten	Pflichtfeld
loc_id	Standort	Zuweisung des Benutzers zu einem Standort Zuordnung der App-Inhalte Zuordnung von Benutzern erstellten Inhalten	Optionales Feld
partner_id	Identifikator des Gesundheitspartners	Zuweisung zu einem Gesundheitspartner Zuordnung der App-Inhalte	Automatisch generiert Ergibt sich aus dem angegeben Webcode
occupation_id	Bereich innerhalb des Unternehmens	Zuweisung des Benutzers zu einem Bereich Zuordnung der App-Inhalte	Pflichtfeld
is_admin	Administratoren Status	Autorisierung des Benutzers	Wird bei Bedarf von Topfit Administratoren gesetzt

Attribut	Klarname	Zweck der Datenverarbeitung	Attributtyp
is_content_admin	Content-Administratoren Status	Autorisierung des Benutzers	Wird bei Bedarf von Topfit Administratoren gesetzt
data	Daten	Optionale Anmeldeparameter des Benutzers zur weiteren Zuweisung	Optionales Feld
newsletter_id	Identifikator für Newsletter Zustellung	Zuordnung zu Newsletter	Optionales Feld
deleted_at	Gelöscht am	Wird bei der Löschung des Benutzerprofils befüllt	Automatisch generiert
created_at	Erstellt am	Wird bei Erstellung des Benutzerprofils befüllt	Automatisch generiert
updated_at	Aktualisiert am	Wird bei Aktualisierung des Benutzerprofils befüllt	Automatisch generiert
external_provider	Identity Provider	Identity Provider für Anmeldeverfahren im SAML- oder OAuth-Standard	Optionales Feld
external_id	Benutzerkennung beim Identity Provider	Einzigartige Benutzerkennung beim Identity Provider	Optionales Feld

2.4.2 Welche Bestandsdaten (vgl. § 14 Abs. 1 TMG) werden von der Web-Applikation automatisch verarbeitet?

- E-Mail-Adresse
- Teilnahme an nationalen Challenges
- Teilnahme an persönlichen Challenges

2.4.3 Welche Inhaltsdaten werden von der Web-Applikation automatisch verarbeitet?

Felder in Geschäftsangaben:

Attribut	**Klarname**	**Zweck der Datenverarbeitung**	**Attributtyp**
business_unit_id	Strategische Geschäftseinheit	Zuweisung des Benutzers zu einer Strategischen Geschäftseinheit Zuordnung der App-Inhalte Zuordnung von Benutzern erstellenten Inhalte	Optionales Feld
region_id	Region	Zuweisung des Benutzers zu einer Region Zuordnung der App-Inhalte Zuordnung von Benutzern erstellenten Inhalte	Optionales Feld
occupation_id	Bereich innerhalb der Strategischen Geschäftseinheit	Zuweisung des Benutzers zu einem Bereich Zuordnung der App-Inhalte	Optionales Feld
loc_id	Standort	Zuweisung des Benutzers zu einem Standort Zuordnung der App-Inhalte Zuordnung von Benutzern erstellten Inhalten	Optionales Feld
occupation	Tätigkeit	Zuordnung der App-Inhalte	Optionales Feld

Weitere Daten, die vom Benutzer bei der Benutzung der Web-Applikation eingegeben werden:

- Kommentare im Dashboard Feed
- Reaktionen im Dashboard Feed
- Kommentare im Challenge Feed
- Reaktionen im Challenge Feed

2.4.4 Welche Verkehrsdaten werden von der Web-Applikation automatisch verarbeitet?

- Angesehene Kurse, Lektionen, Kapitel sowie Seiten in Kursen, bei Videos und E-Learning den Zwischenstand
- Favoriten (markierte Inhalte)
- Kommentare im Dashboard Feed
- Reaktionen im Dashboard Feed
- Kommentare im Challenge Feed
- Reaktionen im Challenge Feed

2.4.5 Werden besondere Arten von personenbezogene Daten oder sensible personenbezogene Daten verarbeitet? Nein.

2.5 Zugangsdaten

(vgl. auch § 13 Abs. 4 TMG)

Besteht die Möglichkeit einer Registrierung und Anmeldung in der Web-App / Webseite mit eigenen Zugangsdaten (Benutzername und Passwort)?

Ja, für die Registrierung und Anmeldung werden folgende Daten genutzt:

Attribut	**Klarname**	**Zweck der Datenverarbeitung**	**Attributtyp**
username	Benutzername	Einmalige, eindeutige Benutzerkennung	Automatisch generiert Ergibt sich aus dem angegeben Webcode
salutation	Anrede	Personalisierte Ansprache des Benutzers	Optionales Feld
firstname	Vorname	Personalisierte Ansprache des Benutzers Anzeige im Chat Anzeige bei Kommentaren	Optionales Feld

		Anzeige bei Reaktionen Anzeige in Posts	

Attribut	**Klarname**	**Zweck der Datenverarbeitung**	**Attributtyp**
lastname	Zuname	Personalisierte Ansprache des Benutzers Anzeige im Chat Anzeige bei Kommentaren Anzeige bei Reaktionen Anzeige in Posts	Optionales Feld
email	E-Mail-Adresse	Nachweis der Authentizität des Benutzers Verifizierung des Benutzers Kommunikation von Terminvergaben	Pflichtfeld
password	Kennwort	Authentifizierung des Benutzers	Pflichtfeld Das Benutzerkennwort durchläuft eine Hashfunktion (Bcrypt)
client_id	Mandant	Zuweisung des Benutzers zum Mandanten Zuordnung der App-Inhalte Zuordnung von Benutzern erstellenten Inhalte	Automatisch generiert Ergibt sich aus dem angegeben Webcode

Attribut	Klarname	Zweck der Datenverarbeitung	Attributtyp
business_unit_id	Strategische Geschäftseinheit	Zuweisung des Benutzers zu einer Strategischen Geschäftseinheit Zuordnung der App-Inhalte Zuordnung von Benutzern erstellenten Inhalte	Pflichtfeld
region_id	Region	Zuweisung des Benutzers zu einer Region Zuordnung der App-Inhalte Zuordnung von Benutzern erstellenten Inhalte	Pflichtfeld
occupation_id	Bereich innerhalb des Unternehmens	Zuweisung des Benutzers zu einem Bereich Zuordnung der App-Inhalte	Pflichtfeld

2.6 Datenexport und Tracking

Ein Datenexport kann von jedem Benutzer mit einer der folgenden Rollen durchgeführt werden:

- Admin (ausschließlich Mitarbeiter der Topfit GmbH)
- Content-Admin (ausschließlich Mitarbeiter der Topfit GmbH)
- Client-Admin (Mandantenebene)
- Business-Unit-Admin (Mandantenebene)
- Region-Admin (Mandantenebene)
- Partner-Admin (Mandantenebene)

Ein Datenexport ist dahingehend beschränkt, dass jeder Benutzer nur die Daten exportieren kann, die er auch selbst anlegen, bearbeiten oder löschen kann.

Das Tracking der Web-Applikation/Website erfolgt mittels Google Analytics. Die Verwaltung und Nutzung des Google Analytics Kontos obliegt der Topfit GmbH.

2.7 Datenempfänger

Web-App/Webseiten Nutzer selbst bzw. die Nutzer untereinander, im vorgesehenen Rahmen der Anwendung.

2.8 Löschkonzept

Automatische Löschungen von Backups erfolgen nach 14 Tagen.

Aufrufen von Löschfunktionen erfolgt auf Anfrage der Mandanten oder deren Benutzer durch die Topfit GmbH. Der Benutzer kann sein Konto selbstständig löschen. Dabei werden der Benutzeraccount, alle benutzerbezogenen Daten, Kommentare und Reaktionen unwiderruflich gelöscht.

Benutzerkonten werden nach 5 Jahren Inaktivität (kein Login) automatisch gelöscht. User erhalten 4 Wochen vorher eine E-Mail, die dieses ankündigt.

Daten, die im Rahmen der Buchung von Terminen erhoben werden, werden automatisch nach 10 Jahren gelöscht.

2.9 Datenschutz im Entwicklungsprozess

Die Entwicklung erfolgt nach dem Secure Development Lifecycle (SDL). Der SDL ist ein systematischer Ansatz zur Integration von Sicherheits- und Datenschutzpraktiken in dem gesamten Softwareentwicklungsprozess.

Die Integration von SDL in unser Datenschutzkonzept umfasst Sensibilisierung und Schulung, Anforderungsanalyse, Risikobewertung, Sicherheits- und Datenschutzdesign, Implementierung, Testen, Überwachung, Aktualisierung und Dokumentation. Durch die Umsetzung des SDL fördern wir eine datenschutzfreundliche Entwicklung und gewährleisten die Einhaltung gesetzlicher Vorschriften und Kundenanforderungen.

3 Technisch-organisatorische Maßnahmen (TOMs)

3.1 Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt.

- Zutrittsregelung für betriebsfremde Personen
- Protokollierung von Besuchern und externen Dienstleistern
- Zentraler Empfangsbereich vorhanden

- Aufenthalt betriebsfremder Personen nur in Anwesenheit von Mitarbeitern
- Gebäudeüberwachung durch Video*
- Maßnahmen zur Objektsicherung bei Fenstern*
- Automatische Türsicherungen*
- Manuelles Schließsystem
- Festgelegte Serverraum-Zutrittsberechtigungen einschl. Schlüsselregelung und Zutrittsprotokollierung*

3.2 Zugangskontrolle

Es wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Authentifikation mit individuellem Benutzernamen und Passwort oder gängigem
- Schlüsselverfahren
- Regelung zur Passwortvergabe (Art, Dauer, Sperrung)
- Zuordnen von Benutzerprofilen zu IT-Systemen
- Automatische, passwortgeschützte Rechnersperre
- Regelung für die Löschung von Berechtigungen ausgeschiedener Mitarbeiter
- Verbindliches Verfahren zur Vergabe von Berechtigungen
- Einsatz von Anti-Viren-Software (wo sinnvoll)
- Sicherung interner Netze gegen unberechtigte Zugriffe von extern (Firewall)
- Externer Zugriff auf interne Netze durch VPN-Technologie (wo erforderlich)

3.3 Zugriffskontrolle

Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Erstellung von Benutzerprofilen
- Erstellen eines Berechtigungskonzepts mit differenzierten Berechtigungsstufen
- Dokumentation der Berechtigungen
- Regelung zum Kopieren von Daten
- Protokollierung und datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger

3.4 Weitergabekontrolle

Es wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- Dokumentation von Datenempfängern bei Transport oder Übermittlung
- Dokumentation der Abruf- und Übermittlungsprogramme
- Führen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Automatische Sperre bei mehrmaliger fehlerhafter Authentifizierung
- Bei physischem Transport sichere Transportbehälter/-verpackungen
- Datenschutzgerechte Vernichtung von Datenträgern

3.5 Weitergabekontrolle

Es wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines
- Berechtigungskonzepts
- Übersicht, mit welchen Applikationen Daten eingegeben, geändert oder gelöscht werden
- können
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen
- übernommen werden
- Löschungsregelung für Protokolldaten

3.6 Auftragskontrolle

Es wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Kontrolle der Datensicherheitsvorkehrungen und schriftlicher Nachweis
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf Vertraulichkeit der Daten gem. Art. 5 Abs. 1 DSGVO
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

3.7 Verfügbarkeitskontrolle

Es wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Notfallkonzept bei IT-Störungen vorhanden
- Redundante Absicherung von Servern und Datenbeständen
- Unterbrechungsfreie Stromversorgung (USV) in Serverräumen*
- (Redundante) Klimaanlage in Serverräumen*
- Automatische Feuer- und Rauchmeldeanlagen*
- Feuerlöscheinrichtungen im Serverraum*
- Alarmmeldungen bei unberechtigten Zutritten zu Serverräumen*
- Sicherungs- und Wiederherstellungskonzept von Daten*

- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort*
- Rekonstruktion von Datenbeständen und Test der Datenbestände*
- Richtlinien zur Wartung und Durchführung von Updates
- Automatisches und permanentes Monitoring zur Erkennung von Störungen
- Regelmäßige Penetrationstests der Anwendung

3.8 Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Logische Mandantentrennung
- Berechtigungskonzept mit Festlegung der Zugriffsrechte
- Trennung von Produktiv- und Testsystem

*im Rechenzentrum bei AWS

4 Datenschutzerklärung

https://topfit.app/info/privacy-policy

5 Datenschutzbeauftragter

info@topfit.gmbh