Technisch Organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, ist zu verhindern, wobei der Begriff „Zutritt“ räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Die fb research GmbH betreibt ihre Infrastruktur an verschiedenen Standorten:

1.) Rechenzentrum beim Betreiber „htp“ (https://www.htp.net/rechenzentrum-it-sicherheit)

Die Zutrittsregelung unterliegt dem Betreiber des Rechenzentrums. Es wird zwischen autorisierten und autorisierenden Personen unterschieden. Die autorisierten Personen erhalten nach der Sicherheitseinführung von htp einen Token, eine PIN Nummer und die Freigabe über einen Fingerabdruckleser. Der Zutritt zum Rechenzentrum unterliegt der Freigabe der autorisierenden Person für erlaubte Zeiten, Schrankzugriffe u.a.

Das Rechenzentrum selbst hat drei Sicherheitsbereiche: Außenanlage mit Parkplatz welcher nur mit dem Token genutzt werden kann. Der zweite Sicherheitsbereich befindet sich hinter der ersten Personenschleuse an welcher auch die Alarmanlage deaktiviert wird. Dieser Sicherheitsbereich ist umfassend Video überwacht. Das eigentliche Rechenzentrum befindet sich hinter der zweiten Personenschleuse die eine zwingende Separation der Personen vorgibt (Lichtschranken und Fingerabdruckleser im Schleusenbereich). Mitgeführte Materialien müssen parallel dazu durch die kameraüberwachte Materialschleuse in den Kernbereich überführt werden. Die Serverräume liegen unter der Erde die nach der zweiten Personenschleuse über eine Treppe erreicht werden. Eine selbstverantwortliche Mitnahme von Dritten ist nicht möglich.

Dieses Rechenzentrum ist nach der Prüfungsnorm: ISO/IEC 27001:2013 bis zum 30.10.2025 zertifiziert. Das Zertifikat hat die Registriernummer: 01 153 1401987

2.) Hauptzentrale der fb research GmbH

Die Firmenräume sind durch eine Alarmanlage und Sicherheitsschlösser abgesichert. Der Serverraum ist gesondert durch eine einbruchgesicherte Tür mit gesonderter Schließanlage gesichert. Schlüssel zu dem Serverraum haben nur die Administratoren und die Geschäftsführung.

3.) Angemietete Infrastruktur bei hetzner (www.hetzner.de)

Dieser Standort dient für das Verfügbarkeitsmonitoring der von der fb research GmbH betriebenen Services und unterliegt keinem besonderen Schutzniveau da keine personenbezogenen Daten im Sinne der DSGVO dort verarbeitet werden. Weiterhin werden hier die reinen Homepages der diversen Domains (z.B. www.fb-research.de, www.vers-award.de etc.) gehostet welche keine personenbezogenen Daten im Sinne der DSGVO verarbeiten oder speichern.

Zugangskontrolle

Das Eindringen Unbefugter in die Datenverarbeitungssysteme ist zu verhindern. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Alle Komponenten der Infrastruktur sind durch Beschränkungen der Zugangswege und Usernamen/Passwörter abgesichert. Direkten Zugang zu den Servern haben ausschließlich die Administratoren und mit reduzierten Berechtigungen die Releasemanager. Administrativer Zugang ist nur für Computer aus der Hauptzentrale über VPN möglich.

Alle von der fb research GmbH betriebenen Services sind durch Firewalls abgesichert welche alle Zugriffswege außer http/https gegen "Welt" sperren.

Ein Datenaustausch über „Hardware“ mit Kunden ist nicht vorgesehen.

Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Die fb research GmbH arbeitet über alle Bereiche mit rollenbasierten Zugriffsrechten. Durch die strikte Trennung von Kunde, Fachbereich, Service, Entwicklung und Administration wird sichergestellt dass niemand auf Daten zugreifen kann auf die kein Zugriff erforderlich ist. Nutzer der Anwendungen haben grundsätzlich nur die Berechtigung auf ihre eigenen Daten zuzugreifen.

Kunden sowohl Mitarbeiter identifizieren sich über Username/Passwort. Bei Integration der Schnittstellen der angebotenen Services kann die Useridentifikation auf das aufrufende System übertragen werden. In diesem Fall ist der Zugriff zusätzlich zum eigenen Usernamen auf den Userbereich des aufrufenden Systems eingeschränkt.

Der Zugriff von Anwendern der Services geschieht einzig über Webbrowser und hat daher keinen Kontakt zu angeschlossener Hardware der fb research GmbH.

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Soweit nicht anders mit dem Kunden vereinbart, werden alle Daten der fb research-Anwendungen in denselben Systemen gehalten. Die Datentrennung erfolgt durch eine logische Trennung der Mandanten und Services auf Basis von Berechtigungen im Bereich Datenbankzugriffe und Zugriffe auf Dateiebene.

Alle Server haben dedizierte Aufgaben, so sind z.B. die Datenbankserver von den Webservern getrennt.

Für alle Systeme gibt es Entwicklungs- und Testsysteme die einen getrennten Weiterentwicklungsworkflow ermöglichen.

Alle Services derfb research GmbH haben eigene Berechtigungen mit der dazugehörigen Trennung der Datenbanken soweit möglich.

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

Pseudonymisierung

- Protokolldateien der Services haben ausschließlich eine ID zur Unterscheidung der Lizenznehmer.
- Endkundendaten werden generell nicht in Logdateien gehalten.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Um ein unbefugtes Lesen zu verhindern kommunizieren alle von der fb research GmbH betriebenen Services über TLS-verschlüsselte Kommunikationswege. Die Hauptzentrale ist über ein AES256 verschlüsseltes VPN mit den Rechenzentren verbunden. Der Mailversand der Services erfolgt über einen selbst betriebenen SMTP-Relayhost. Aus Sicherheitsgründen ist der Relayhost nur intern erreichbar und steht somit nur den eigenen Services zur Verfügung. Optional steht eine S/MIME Verschlüsselung für einzelne Empfangsadressen oder ganze Zieldomänen zur Verfügung.

Backups verbleiben an den Standorten wo sie erstellt wurden, jedoch auf getrennten Systemen.

Defekte Festplatten und anderer permanenter Speicher werden datenschutzkonform von externen Unternehmen vernichtet. Der Transport geschieht in abgeschlossenen Behältern im Vier-Augen-Prinzip.

Externe Speichermedien wie z.B. USB-Sticks, DVD RW, Online-Speicherdienste sind für alle Mitarbeiter deaktiviert und müssen nach Bedarfsprüfung einzeln durch die Administration frei gegeben werden.

Ein Austausch von Daten mit Kunden per „Hardware“ ist nicht vorgesehen.

Externe Dienstleister haben keine eigenen Zugänge zu den Systemen und stehen damit immer unter Aufsicht der Administratoren.

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und –pflege sind zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Alle Aktivitäten des Kundenservice der fb research GmbH werden bei den entsprechenden Kunden vermerkt. Diese Logdaten können nicht von den Mitarbeitern nachträglich bearbeitet werden.

Die Lizenznehmer selbst haben ausschließlich Zugriff auf ihre Kunden. Eine Bearbeitung dieser personenbezogenen Daten durch Dritte ist nicht vorgesehen und wird programmtechnisch nicht unterstützt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch):

Folgende Maßnahmen werden ergriffen:

Die zum Betrieb der Services notwendigen Systeme werden ausschließlich in den Rechenzentren gehostet die einem permanenten Monitoring unterliegen. Dabei werden nicht nur die reinen Verfügbarkeitsdaten geprüft sondern auch Performancedaten die eine mögliche Früherkennung von Problemen ermöglichen.

Alle Rechenzentren betreiben eine Notstromanlage, welche die Infrastruktur gegen Stromausfall und andere Risiken wie z.B. Überspannungsschäden absichert. Zudem sind in allen Rechenzentren Brandschutz- und Klimaanlagen installiert.

Die Systeme selbst stehen redundant zur Verfügung und werden über ein automatisches Deploysystem aktualisiert.

Alle Server arbeiten auf hochverfügbaren Festplattenspeicher, der von einem Unified Storagesystem zur Verfügung gestellt wird.

Um den Anforderungen an einen umfassenden Schutz vor Virenbefall sicher zu stellen, hat die fb research GmbH einen mehrstufigen Virenschutz implementiert, um die verschiedenen Eingangskanäle abgesichert zu haben.

- Der eingehende Mailverkehr wird über zwei unabhängige Systeme geprüft.
- Externe Medien sind global deaktiviert und können nur durch die Administration freigegeben werden.
- Auf jedem Arbeitsplatz ist eine zentral verwaltete Endpointsecurity installiert, die nur durch die Administration deaktiviert werden kann.
- Zudem überprüft die eingesetzte Firewall den Traffic auf bekannte Bedrohungen.

Von allen Datenbanksystemen werden täglich Datensicherungen durchgeführt und getrennt aufbewahrt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management;

- Der vertragsgegenständliche Service wurde bereits im Design auf Datenschutzprinzipen ausgerichtet.
- Alle Funktionserweiterungen durchlaufen einen strengen Prozeß zur Implementierung, der auch die DSGVO beachtet.
- Alle Serverlogdateien werden regelmäßig gesichtet, ob und welche Informationen bei Systemfehlern protokolliert werden.

Incident-Response-Management (Art. 33 Abs. 1 DSGVO);

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragnehmer unverzüglich, nachdem ihm die Verletzung bekannt wurde, diese der verantwortlichen Stelle oder im Falle einer eigenverantwortlichen Arbeit gemäß Art. 55 DSGVO der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung nicht binnen 72 Stunden, fügt der Auftragnehmer eine Begründung für die Verzögerung bei.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Alle Services erheben nur die Daten die für den Betrieb der Services notwendig sind. Eine toolspezifische Auflistung kann in den Leistungsbeschreibungen eingesehen werden (Link).

Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Unterauftraggeber:

Die Arbeitsabläufe der Services sind fest vorgegeben und können nur im vorgegebenen Rahmen beeinflusst werden. Der Umfang der zur Verfügung stehen Möglichkeiten sind im Vorfeld mit dem Auftraggeber abgestimmt.

Alle Arbeiten des Kundenservices werden im direkten Dialog mit dem Auftraggeber durchgeführt. Eine Kontrolle findet im direkten Anschluss der Arbeiten über den Zugriff auf die Onlineservices statt.

Sofern eigene Auftragnehmer eingesetzt werden, schließt der Auftragnehmer mit diesen seinerseits Auftragsdatenverarbeitungsverträge, in Übereinstimmung mit seinen Auftragsgebern, ab.