Informationssicherheit und Datenschutz

Inhalt

1. Datenfluss innerhalb der atwork Suite

1.1 Übersicht Softwarekomponenten:

In der nachstehenden Abbildung sind alle Softwarekomponenten ("Tools") und Datenflüsse für die Bereitstellung der verschiedenen Dienste abgebildet. Innerhalb dieser Teile werden die Daten wie nachfolgend beschrieben verwendet, um die vertraglich vereinbarten Dienste bereitzustellen.

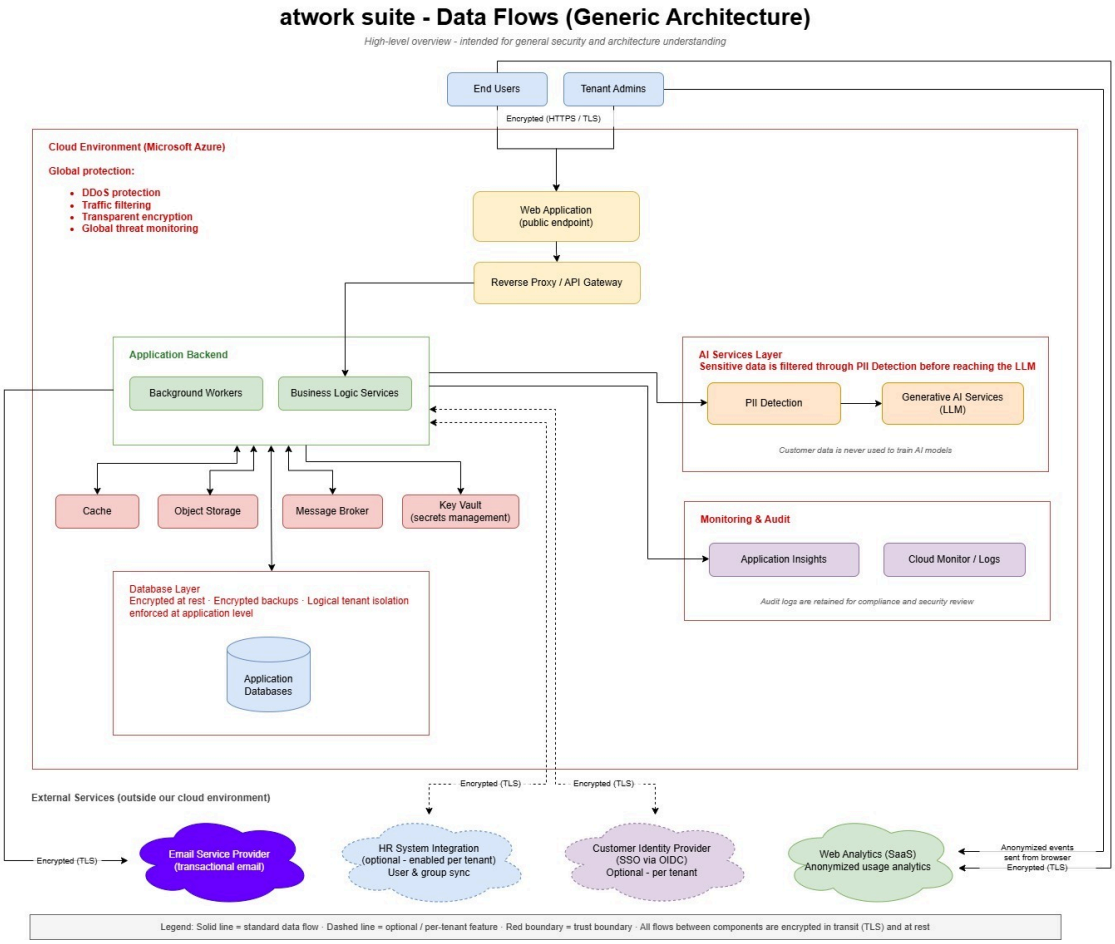


Abbildung 1: Data flow

1.2 Architektur und Einsatz

1.2.1 Proprietäre Anwendung

Die atwork-Anwendung ermöglicht die Erstellung von Mitarbeiterumfragen, welche mittels künstlicher Intelligenz ausgewertet werden können. Dazu werden Daten über Eingabe- und Informationsfelder erfasst, was eine klare Trennung von Datenkategorien ermöglicht. In der Datenbank definierte Eingabe- und Informationsfelder ("Fields") werden im Folgenden durch Kursivschrift hervorgehoben z.B. *First Name.*

Das Frontend wird mit **Angular** entwickelt und das Backend mit **.NET**, wobei eine moderne Architektur zum Einsatz kommt, die die Verantwortlichkeiten trennt und die Sicherheit erhöht.

Die Webanwendung wird auf **Microsoft Azure** gehostet und nutzt damit eine zuverlässige und skalierbare Cloud-Infrastruktur. Die Microsoft Azure Server befinden sich in der Schweiz.

Der einzige Datenfluss, bei dem die Azure-Umgebung verlassen wird, ist für die User Anmeldung via AWS. Weitere Informationen dazu finden sich unten.

1.2.2 Microsoft Azure Service

Zu den genutzten Diensten in der Azure-Umgebung gehören:

- **App Services** für die Anwendungslogik.
- **Datenbanken** mit nativer Verschlüsselung für eine sichere Speicherung.
- **Speicherkonten** für die Verwaltung zusätzlicher Ressourcen.
- **Redis Cache** zur Optimierung der Leistung und sicheren Verwaltung temporärer Daten.
- **Language Services** für alle erforderlichen Sprachverarbeitungsaufgaben, wie z. B. Textanalyse oder Übersetzungen, mit Datenverarbeitung unter Einhaltung strenger Sicherheitsstandards.
- **Message Brokers**, um eine sichere und zuverlässige Kommunikation zwischen den verschiedenen Komponenten des Systems zu gewährleisten.
- **Azure OpenAI Service,** als sichere LLM Integration (vergleiche Kapitel 5 «Detailbeschreibung Integration Azure OpenAI Service».

Sichere Konfiguration der Azure-Infrastruktur

- Wir gewährleisten die Sicherheit unseres Azure-Mandanten und unserer Infrastruktur, indem wir die bewährten Verfahren und Compliance-Richtlinien von Azure befolgen:
    - Azure Policy wird verwendet, um Sicherheitskonfigurationen durchzusetzen und Fehlkonfigurationen zu verhindern.
    - Die rollenbasierte Zugriffssteuerung (RBAC) beschränkt den Zugriff nach dem Prinzip der geringsten Privilegien.
    - Best Practices für die Netzwerksicherheit werden angewendet, um unbefugten Zugriff einzuschränken.

Wir halten unsere Azure-Dienste und -Abhängigkeiten auf dem neuesten Stand, um Sicherheitsrisiken zu reduzieren.

1.2.3 AWS Simple Email Service

Der erste Zugang zur Lösung von atwork erfolgt über einen einmaligen Link, welcher per E-Mail über den AWS Simple Email Service ("AWS SES") versendet wird. Weitere Informationen über die Sicherheit von AWS SES finden Sie hier.

Sichere Konfiguration von Schnittstellen mit AWS

Für die Verbindungen zwischen unserer Anwendung und AWS befolgen wir bewährte Sicherheits-verfahren, um sichere Interaktionen zu gewährleisten:

- Sichere API-Schlüsselverwaltung: API-Schlüssel und Anmeldedaten werden sicher gespeichert und folgen bewährten Verfahren zur Zugriffskontrolle.
- Kundenspezifische Konfiguration: In unserem Verwaltungsportal, auf das nur ausgewählte atwork-Mitarbeiter mit bestimmten Berechtigungen (Customer Success, IT) Zugriff haben, können die E-Mail-Zustellungseinstellungen jedes Mandanten verwaltet werden. Endkunden haben keinen Zugriff auf diesen Bereich. Für jeden Mandanten können die folgenden Parameter konfiguriert werden: Mail-Host, Mail-Port, Mail-Absenderadresse, Mail-Absendername, Mail-Benutzername und Mail-Passwort. Diese Einstellungen gelten für alle ausgehenden E-Mails dieses Mandanten. Die Anmeldedaten können von autorisierten atwork-Mitarbeitern eingesehen und aktualisiert werden, wenn dies für den Kundensupport oder die Wartung erforderlich ist. Alle Werte werden in einer von Azure gehosteten Datenbank gespeichert und durch Azure-verwaltete Verschlüsselung im Ruhezustand geschützt. Während der E-Mail-Zustellung ruft das Backend die Werte dynamisch zur Laufzeit ab; es werden keine Anmeldedaten fest codiert oder in statischen Konfigurationsdateien gespeichert. Der Zugriff auf diese Anmeldedaten ist streng auf atwork-Mitarbeiter mit einem betrieblichen Bedarf beschränkt, und die Trennung zwischen Mandanten wird durch logische Isolierung auf Datenbankebene gewährleistet, wodurch eine mandantenübergreifende Offenlegung verhindert wird.
- SMTP-Anmeldedaten werden in unserer Anwendungsdatenbank gespeichert, die in Microsoft Azure gehostet wird. Die Datenbank wird im Ruhezustand mit den Standardverschlüsselungsmechanismen von Azure verschlüsselt, die von Azure selbst verwaltet werden. Dadurch wird sichergestellt, dass alle gespeicherten Daten, einschliesslich der SMTP-Anmeldedaten, standardmässig verschlüsselt sind, ohne dass eine manuelle Schlüsselverwaltung erforderlich ist.
- Verschlüsselte Kommunikation: Alle zwischen unserer Anwendung und AWS übertragenen Daten werden mit TLS 1.2 verschlüsselt.
- Zugriff mit geringsten Rechten: Berechtigungen sind auf das für die Funktionalität erforderliche Minimum beschränkt.
- Zugriffskontrolle: Auf die Anmeldedaten können nur Backend-Dienste zugreifen, die für den Versand von E-Mails zuständig sind, sowie Benutzer mit entsprechenden Konfigurationsrechten innerhalb der Anwendung. Sie werden niemals Endbenutzern ohne die erforderlichen Berechtigungen oder dem Frontend zugänglich gemacht.
- Keine Hardcoding: SMTP-Anmeldedaten werden niemals im Quellcode oder in statischen Konfigurationsdateien fest codiert. Sie werden immer sicher zur Laufzeit abgerufen.
- Auditing und Überwachung: Eine spezifische Überwachung oder Kontrolle des Zugriffs auf diese Einstellungen ist derzeit über die standardmässigen Schutzmassnahmen auf Plattformebene hinaus nicht implementiert.

2 Überblick über die Systemsicherheit

2.1 Sichere Entwicklung

atwork befolgt bewährte Verfahren und Branchenstandards, um die sichere Entwicklung der Anwendung zu gewährleisten. Insbesondere befolgt atwork die OWASP Top Ten-Guidelines, um häufige Web-Sicherheitsrisiken wie SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) und Insecure Deserialization zu minimieren.

Unsere Sicherheitspraktiken umfassen:

- Code-Reviews und sichere Secure Coding-Praktiken: Entwickler befolgen sichere Secure Coding-Prinzipien und führen Peer-Code-Reviews durch, um potenzielle Sicherheitslücken zu identifizieren.
- Static Code-Analyse: Wir verwenden automatisierte Tools, um Sicherheitsprobleme in unserer Codebasis frühzeitig im Entwicklungsprozess zu erkennen.
- Regelmässige Updates und Patches: atwork stellt sicher, dass die proprietäre Anwendung durch regelmässige Entwicklungszyklen auf dem neuesten Stand bleibt. Dabei überprüfen und aktualisieren wir in regelmässigen Abständen Abhängigkeiten, wenden Sicherheitspatches an und befolgen bewährte Verfahren, um eine sichere und unterstützte Version zu erhalten
- Dependency Management: Wir aktualisieren unsere Abhängigkeiten regelmässig, um sicherzustellen, dass wir die neuesten stabilen und sicheren Versionen verwenden. Azure Update Manager und Azure Security Center überwachen und verwalten Updates für die zugrunde liegende Infrastruktur, Betriebssysteme und in unserer Umgebung verwendete Software von Drittanbietern.
- Authentifizierung und Autorisierung: Wir implementieren sichere Authentifizierungsmechanismen, setzen strenge Passwortrichtlinien durch und verwenden eine rollenbasierte Zugriffskontrolle (RBAC).
- Verschlüsselung und Datenschutz: Sensible Daten werden während der Übertragung mit TLS verschlüsselt und sicher gespeichert.
- Sicherheitstests: Unser Entwicklungsprozess umfasst sowohl Unit- als auch Integrationstests, und wir führen regelmässig Penetrationstests durch.
- Prinzip der geringsten Privilegien: Wir befolgen das Prinzip der geringsten Privilegien für den Datenbankzugriff, API-Schlüssel und Berechtigungen für die Cloud-Infrastruktur.
- Protokollierung und Überwachung: Wir führen Protokolle für sicherheitsrelevante Ereignisse und überwachen unsere Anwendung aktiv auf Anomalien.

Diese Verfahren helfen uns, eine sichere Anwendung zu erstellen und zu warten, während wir gleichzeitig unsere Sicherheitslage kontinuierlich verbessern.

2.2 Verschlüsselung bzgl. AWS

- Der erste Zugang erfolgt über einen einmaligen Link per E-Mail (über AWS SES).
    - Für Kunde X bedeutet dies, dass Zugriffsberechtigungen nur über E-Mail-Adressen eingerichtet werden können, die ein Admin in Form eines User Profils anlegt. Typischerweise werden *First Name, Last Name* und *E-Mail Address* vom Admin erfasst und die weiteren Informationen vom User ergänzt. Ein Admin könnte aber alle Informationen von Tabelle 1 erfassen. An AWS werden nur die Fields *First Name, Last Name*, *E-Mail Address* und ein Hyperlink um ein Passwort festzulegen gesendet.
    - Die Anwendung verbindet sich über SMTP über STARTTLS mit AWS SES. Dabei wird eine benutzerdefinierte verifizierte Domain für ausgehende E-Mails verwendet, wobei SPF, DKIM (2048 Bit) und DMARC konfiguriert sind. Die DKIM-Signatur ist aktiviert und aktiv.
- **Daten bei der Übertragung**:
    - Die gesamte Kommunikation zwischen den Clients und dem Server ist durch **HTTPS** und **TLS 1.2** gesichert, wodurch die Vertraulichkeit und Authentizität der Daten bei der Übertragung gewährleistet ist.
    - Alle Übertragungen werden nach Möglichkeit während der Übertragung verschlüsselt, und die Authentifizierung auf Domain-Ebene gewährleistet die Integrität der Nachrichten und schützt vor Spoofing
- **Daten im Ruhezustand**:
    - Die Datenbanken werden mit den in integrierten Verschlüsselungsfunktionen von Azure verschlüsselt.
    - Die Verschlüsselungsschlüssel zum Schutz der gespeicherten Daten in unseren Azure-Datenbanken werden von Microsoft mithilfe von dienstverwalteten Schlüsseln (von Microsoft verwalteten Schlüsseln) verwaltet.
    - Microsoft übernimmt die Speicherung, Zugriffskontrolle, Rotation und den Schutz der Schlüssel als Teil der integrierten Sicherheit der Azure-Plattform.
    - Der Zugriff auf diese Schlüssel wird von Microsoft gemäss den branchenüblichen Best Practices und Compliance-Standards streng kontrolliert und überwacht. atworks hat keinen direkten Zugriff auf die Verschlüsselungsschlüssel selbst.

2.3 Beschreibung Datenbearbeitung und Datenschutz

Die Anwendung ist für die Verwaltung von Mitarbeiterbefragungen, Massnahmen und Wirkungsmanagement für Kundenunternehmen konzipiert.

Die Anwendung verarbeitet die folgenden Kategorien von personenbezogenen Daten, welche detaillierter in den Tabellen 1-3 im Anhang dargestellt werden:

- Vorname und/oder Familienname
- Kontaktangaben
- Personalverwaltung
- Personaldaten
- Daten zur Qualifizierung
- Beurteilung der Mitarbeiter

Ausserdem werden die Antworten der User (d.h. der Mitarbeiter des Kunden X, die die Umfragen ausfüllen) verarbeitet, welche ebenfalls personenbezogene Daten enthalten können. atwork kann nicht sicherstellen, dass die User keine sensiblen Daten (z. B. besondere Datenkategorien) in die Umfrage eingeben; dies muss auf operativer Ebene vom Kunden X sichergestellt werden, wenn dies gewünscht wird. atwork steht weiterhin zur Verfügung, um die User bei der Schulung im Umgang mit der Plattform zu unterstützen.

Angesichts der Sensibilität der verarbeiteten Informationen setzt atwork verschiedene Sicherheitsmassnahmen ein, um den Schutz der Daten zu gewährleisten. Insbesondere verlassen Inhalte der designierten PII-Fields die Azure-Umgebung nicht. Um die Sicherheit weiter zu erhöhen, werden die Texteingaben, die an Azure OpenAI Service gesendet werden, durch das Tool Azure AI Language PII Detection bereinigt. Dies stellt eine zusätzliche Sicherheitsschicht dar.
Vertraglich verpflichtet atwork seine Unterauftragnehmer zur Einhaltung der datenschutzrechtlichen Vorschriften von der anwendbaren Datenschutzgesetze. atwork stellt sicher, dass sämtliche Datentransfers durch genügende rechtliche Vereinbarungen abgedeckt sind.

2.4 Schutz vor Schwachstellen

- In regelmässigen Abständen **werden Codeüberprüfungen** durchgeführt, um potenzielle Sicherheitslücken zu ermitteln und zu beheben.
- Hinsichtlich dem Azure OpenAI-Dienst
    - Die Anwendung greift über interne, serverseitige API-Aufrufe auf den Azure OpenAI-Dienst zu. Die Authentifizierung erfolgt über Azure Active Directory (AAD) unter Verwendung verwalteter Identitäten, wobei der Zugriff auf den Dienst durch rollenbasierte Zugriffssteuerung (RBAC) eingeschränkt und verwaltet wird. Die gesamte Kommunikation mit dem Dienst erfolgt über HTTPS unter Verwendung von TLS 1.2, wodurch die Vertraulichkeit und Integrität der übertragenen Daten gewährleistet ist.
    - Azure wendet eine standardmässige Datenaufbewahrungsrichtlinie für den OpenAI-Dienst an: Über die API gesendete Eingabeaufforderungen und Vervollständigungen können bis zu 30 Tage lang gespeichert werden, ausschliesslich zum Zweck der Überwachung und Verhinderung von Missbrauch. Diese Protokolle werden nicht zum Trainieren von Modellen verwendet und sind nur autorisierten Microsoft-Mitarbeitern unter strengen Zugriffskontrollen zugänglich. Diese Richtlinie ist von Microsoft hier

dokumentiert: https://learn.microsoft.com/en-us/azure/ai-foundry/responsible-ai/openai/data-privacy?tabs=azure-portal

- Hinsichtlich des AWS Simple Email Services (SES)
  - E-Mails werden von der Anwendung über den AWS Simple E-Mail-Service (SES) unter Verwendung der SMTP-Schnittstelle versendet. Die gesamte Kommunikation über SMTP wird mit STARTTLS verschlüsselt, wodurch eine sichere Übertragung der E-Mail-Daten zwischen der Anwendung und AWS SES gewährleistet ist. Die Authentifizierung erfolgt über SMTP-Anmeldedaten, die aus den AWS-Identity and Access Management (IAM)-Anmeldedaten abgeleitet werden. Diese Anmeldedaten werden sicher gespeichert und sind nicht fest in der Anwendung codiert. Zum Schutz vor Spoofing und Phishing unterstützt und erzwingt SES die Verwendung von Standard-E-Mail-Authentifizierungsprotokollen wie SPF, DKIM und DMARC, die auf Domänenebene konfiguriert werden: Mehr Informationen finden sich hier: https://docs.aws.amazon.com/ses/latest/dg/security.html
- Die Anwendung wird **regelmässigen Penetrationstests** unterzogen, um Schwachstellen zu erkennen und zu beseitigen, bevor sie ausgenutzt werden können.

2.5 Protokollierung und Überwachung

- Der Gesamtstatus der Anwendung (Zustand und die Leistungsmetriken der Anwendung auf höchster Ebene, z. B. die Betriebszeit des Servers, die Antwortzeiten und die Systemverfügbarkeit) wird überwacht. Auf die Protokolldetails wird nur im Falle einer detaillierten Untersuchung eines bestimmten Tickets zugegriffen.
- Diese Überwachung stellt sicher, dass die Anwendung wie erwartet funktioniert und ermöglicht dass, Anomalien oder potenzielle Probleme sofort erkannt werden. Die proaktive Überwachung wird durchgeführt, um die Sicherheit der Anwendung zu gewährleisten und potenzielle Bedrohungen zu erkennen. Im Einzelnen:
  - Proaktive Überwachung: Tools wie Azure Application Insights und Dashboards werden aktiv zur Überwachung der Anwendungsaktivität eingesetzt. Dazu gehören Metriken wie Anfragemuster, Fehlerraten und ungewöhnliche Spitzen im Datenverkehr, die auf potenzielle Probleme oder bösartige Aktivitäten hinweisen können.
    - Alle Systemaktivitäten werden in **Azure Application Insights** protokolliert, was die Verfolgung von Interaktionen und die Analyse von Nutzungsmustern ermöglicht.
    - Wir unterscheiden zwar auf Anwendungsebene nicht ausdrücklich zwischen administrativen und nicht-administrativen Benutzern, aber alle Benutzeraktivitäten werden zentral aufgezeichnet.
    - Atwork-Entwickler Admins nutzen Azure-Dashboards, die so konfiguriert sind, dass sie wichtige Metriken überwachen, Anomalien erkennen und schnell auf potenzielle Sicherheitsvorfälle reagieren

können. Der Zugriff auf diese Protokolle wird durch die rollenbasierte Zugriffskontrolle von Azure streng kontrolliert, und nur autorisierte Mitarbeiter unseres Teams haben Zugriff darauf. Die Protokolldaten werden nur im Falle eines konkreten Vorfalls oder technischen Fehlers überprüft. Es ist wichtig zu beachten, dass falsche Anmeldeversuche allein keine solche Überprüfung auslösen.

  - Sicherheitsprotokolle: In den Protokollen werden detaillierte Informationen über Interaktionen mit der Anwendung erfasst, einschliesslich fehlgeschlagener Anmeldeversuche und anderer Aktivitäten, die auf Angriffsversuche hindeuten könnten. Die Daten in den Protokollen werden zwar anonymisiert, um die Privatsphäre der User zu schützen, aber sie ermöglichen uns dennoch, Muster zu analysieren und auf verdächtiges Verhalten angemessen zu reagieren.
  - Als zusätzliche Sicherheitsmassnahme werden Konten nach fünf fehlgeschlagenen Anmeldeversuchen automatisch für eine Minute gesperrt.
- Kurz gesagt, es gibt einen Mechanismus, um potenzielle Angriffe zu überwachen und darauf zu reagieren, und wir ergreifen proaktive Massnahmen, um die Sicherheit der Anwendung zu gewährleisten.

2.6 Einhaltung von Vorschriften

- Die Verwaltung personenbezogener Daten entspricht den Anforderungen dem **Schweizerischen** Datenschutzgesetz (DSG) und der **Datenschutzgrundverordnung (DSGVO)** sowie der anwendbaren Schweizer kantonalen Datenschutzrichtlinien, einschliesslich:
  - Transparenz bei der Datenverarbeitung.
  - Umsetzung von technischen und organisatorischen Massnahmen zum Schutz personenbezogener Daten.
  - Die Fähigkeit, Anfragen von User bezüglich ihrer Rechte (Zugang, Berichtigung, Löschung usw.) zu bearbeiten.

2.7 Sicherheitsprüfung

- Zusätzlich zu den regelmässigen Penetrationstests werden automatisierte Tools wie SonarCloud als Teil unseres Entwicklungsworkflows eingesetzt. SonarCloud ist als Qualitätskontrolle in jeden Pull-Request integriert, um Sicherheitslücken und Codefehler automatisch zu erkennen.
- Wir führen auch manuelle Codeüberprüfungen durch, wobei der Schwerpunkt auf der Identifizierung potenzieller Probleme vor der Bereitstellung liegt.
- Darüber hinaus verfügen wir über eine umfangreiche Suite von Unit- und Integrationstests für die gesamte Codebasis. Diese sind zwar nicht sicherheitsspezifisch, helfen jedoch dabei, Logikfehler und Regressionen frühzeitig im Entwicklungsprozess zu erkennen und tragen so zur allgemeinen Robustheit der Anwendung bei.

Das Sicherheitssystem der Webanwendung folgt Best Practices und dem aktuellen Stand der Technik und kombiniert robuste Tools und Dienste von Azure mit internen Prüf- und Testverfahren. Dies gewährleistet den Schutz sowohl der persönlichen Daten der User als auch der Umfrageantworten, die Einhaltung gesetzlicher Standards und die Minimierung von Sicherheitsrisiken.

3 Zugriffskontrolle

3.1 Zugriff auf unsere atwork-Webanwendung

3.1.1 Zugangsrollen

Im Folgenden wird zwischen drei Rollen unterschieden:

- **atwork-Entwickler**: atwork-Mitarbeitende, welche Zugriff auf die atwork Lösung haben müssen, um den Betrieb der atwork-Lösung sicherstellen zu können.
- **Admin**: Vom Kunden X bezeichnete Personen mit erweiterten Zugangsrechten (s. unten).
- **User**: einfache Nutzer der atwork-Lösung, in der Regel Mitarbeitende des Kunden X. Nutzer werden von Admins freigeschaltet.

Weitere Details der Zugangsrollen sind den Tabellen im Anhang zu entnehmen.

3.1.2 Zugriffsrechte und Authentisierung atwork-Entwickler

Atwork-Entwickler haben vollumfängliche Zugriffsrechte. Hier werden standardisierte technische und organisatorische Sicherheitsmassnahmen gewahrt, z.B. Mitarbeiterschulung und erhöhte Sicherheitsanforderungen wie Multi-Faktor-Authentifizierung (MFA). Auf die Datenbanken wird nur zweckmässig ("Need-to-Access"), z.B. für Fehlerbehebung oder Prüfung der Logs, zugegriffen.

Diese erhöhten Zugriffsrechte sind notwendig, damit die Dienste von atwork geprüft und weiterentwickelt werden können und die Funktionsfähigkeit sichergestellt ist.

Atwork-Entwickler greifen entweder über das Azure-Portal oder über die Azure-CLI auf die Infrastruktur zu, wobei sie Anmeldeinformationen verwenden, die von Azure Entra ID (ehemals Azure Active Directory) verwaltet werden. Der Zugriff wird durch eine Kombination aus Benutzername/Passwort und MFA geschützt, die für alle Entwickler und Umgebungen (einschliesslich Nicht-Produktionsumgebungen) vorgeschrieben ist.

Der Authentifizierungsprozess funktioniert wie folgt:

- **Benutzername und Passwort**: Alle Entwickler authentifizieren sich über individuelle Benutzerkonten. Diese Konten unterliegen den standardmässigen Cloud-Passwortrichtlinien von Microsoft, die Anforderungen wie eine Mindestlänge von 8 Zeichen, die Verwendung komplexer Zeichen (Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen) und die Vermeidung zuvor verwendeter Passwörter umfassen. Die Gültigkeitsdauer von Passwörtern wird gemäss den aktuellen Sicherheitsempfehlungen von Microsoft nicht erzwungen.
- **Richtlinie zur Kontosperrung**: Azure Entra ID wendet intelligente Sperrrichtlinien zum Schutz vor Brute-Force-Angriffen an. Konten werden nach mehreren

fehlgeschlagenen Anmeldeversuchen innerhalb eines kurzen Zeitraums vorübergehend gesperrt.

- **Multi-Faktor-Authentifizierung (MFA):** MFA wird für alle Entwicklerkonten erzwungen. Benutzer können ihren bevorzugten zweiten Faktor auswählen, z. B. eine Authentifizierungs-App (z. B. Microsoft Authenticator), SMS oder andere unterstützte Methoden. MFA wird direkt über Azure Entra ID verwaltet und gilt für alle Umgebungen.
- **Zugriffsprotokolle:** Azure Entra ID führt detaillierte Protokolle über Authentifizierungsereignisse. Diese Protokolle sind verfügbar und können bei Bedarf überprüft werden, es werden jedoch keine routinemässigen manuellen Überprüfungen der Authentifizierungsereignisse durchgeführt.

3.1.3 Zugriffsrechte und Authentisierung Admins

atwork richtet einem vom Kunden X definierten Administrator auf Seite Kunden X ein Admin-Konto ein, bevor Mitarbeitende Zugriff auf die Applikation erhalten. Der Admin kann dann weitere Nutzer hinzufügen und die Adminrolle ohne weitere Genehmigungsprozesse frei an weitere Benutzer vergeben. .

Zugang zur Anwendung: Der Administrator greift mit einem Benutzernamen und einem Passwort auf die Anwendung zu.

- Aus technischer Sicht sind Admins normale User mit erweiterten Berechtigungen.
- Bei der Erstellung ihres Kontos legen Admins ihr eigenes Passwort fest, das den Passwortrichtlinien der Anwendung entsprechen muss: mindestens 12 Zeichen, darunter mindestens ein Grossbuchstabe, ein Kleinbuchstabe, eine Ziffer und ein Sonderzeichen. Nach fünf fehlgeschlagenen Anmeldeversuchen wird das Konto für eine Minute gesperrt.
- Alle Anmeldeversuche und Benutzeraktionen, einschliesslich derjenigen von Admins, werden mit Application Insights aufgezeichnet. Es gibt jedoch keine Warnmechanismen, die speziell mit sensiblen Verwaltungsaktionen verknüpft sind.
- Die Anwendung unterstützt derzeit keine Multi-Faktor-Authentifizierung (MFA) und es gibt keine kurzfristigen Pläne, diese einzuführen. Als optionale Funktion unterstützt die Anwendung die Integration mit externen Authentifizierungsanbietern auf Kundenbasis. Wenn diese Funktion aktiviert ist, können sich alle Benutzer dieses Kunden (einschliesslich Admins) über den Identitätsanbieter ihrer Organisation, z. B. Azure Entra ID, anmelden. Diese Einstellung wurde für Kunden X nicht aktiviert.

Admin-Rechte: Admins haben umfassendere Zugriffsrechte als User. Sie können:

- User Profile erstellen und bearbeiten. Sie haben Zugriff auf alle Informationen in **Tabelle 1**.
- Admin-Rolle an andere User vergeben.
- Umfragen erstellen, veröffentlichen und verwalten.

- gemäss untenstehenden Einschränkungen auf eingereichte Umfrageantworten von Usern zugreifen (s. Zugangsrechte Admins).

Benutzerrollen und Berechtigungen, einschliesslich Administratorrechten, werden intern innerhalb der Anwendung über ein rollenbasiertes Zugriffsmodell verwaltet.

Zugangsrechte Admin: Admins können gewisse Umfrageresultate aller User einsehen. Hier gilt es zwischen dem gewöhnlichen Modus ("Default Mode") und der Zustimmung zur Identifikation ("Opting-In") zu unterscheiden. Admins können keine persönlich identifizierende Informationen ("PII") in Verbindung mit Umfrageantworten sehen, es sei denn, der betroffene User wählt die Option "Opting-In" oder die Texteingabe des Users beinhaltet identifizierende Informationen:

- Im **Default Mode** werden zwar Umfrageresultate über die *ID* direkt mit dem Profil des Users in der Datenbank gemäss **Tabelle 1** verlinkt, aber aufgrund der Einstellung des Default-Mode kann niemand ausser atwork-Entwicklern mit einem "Need-to-Access" ("atwork-Entwickler") auf die identifizierenden Fields wie *First Name, Last Name* oder *E-Mail Address* zugreifen. Der Admin sieht die Antworten der Umfrage, aber nicht die damit in Verbindung gebrachten User. Die *ID* der User wird dem Admin in keinem Szenario angezeigt. Das *ID* Field verbirgt sich hinter einer logischen Schicht, die im Hintergrund die Assoziierung zur Speicherung in Verbindung mit dem User Profil vornimmt. Nur atwork-Entwickler sehen hinter diese Logische Schicht und können somit die Verbindung der beiden Datenbanken von **Tabelle 1** und **Tabelle 2** oder **Tabelle 3** nachvollziehen.
- Ohne Opting-in liegen die Daten den Admins nur in pseudonymisierter Form vor, ohne dass sie jedoch Zugriff auf den Schlüssel hätten, der ihnen eine Zuordnung der pseudonymisierten Daten zu einer natürlichen Person erlauben würde.

3.1.4 Zugriffsrechte und Authentisierung User

Zugang zur Anwendung: Vergleiche die Ausführungen zu den Admins.

Profilzugriff: User können ihre eigenen Profile einsehen und bearbeiten, einschliesslich aller Felder von **Tabelle 1**.

Umfragen: User haben Zugriff auf Umfragen, die von Admins veröffentlicht wurden. Sie können:

- Umfragen ausfüllen und entscheiden, ob ihre Antworten anonym sein sollen (Default Mode vs. Opting-In).
- ihre eigenen Umfrageantworten einsehen.

Einschränkungen: User haben keinen Zugriff auf die Profile oder Umfrageantworten anderer User.

Authentifizierung und Autorisierung:

- **Authentifizierung über einen einmaligen Link:** Endbenutzer können sich mit einem Benutzernamen und einem Passwort anmelden. Zusätzlich haben sie die Möglichkeit, über einen einmaligen Link an Umfragen teilzunehmen, wodurch sie Antworten einreichen können, ohne sich bei der Anwendung anzumelden. Dieser Link bietet jedoch keinen Zugriff auf die Anwendung selbst und ist nur gültig, solange die Umfrage aktiv und noch nicht abgeschlossen ist.
- **Passwortlänge für Benutzer (Supervisor-Funktion):** Alle Benutzer, einschliesslich derjenigen mit Supervisor-Rolle, müssen Passwörter mit mindestens 12 Zeichen verwenden, darunter mindestens ein Grossbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Sonderzeichen. Damit wird die vereinbarte Mindestlänge von 10 Zeichen vollständig umgesetzt.
- **Zugriffsprotokollierung:** Alle Benutzerzugriffsereignisse werden mit Application Insights protokolliert, wodurch die Rückverfolgbarkeit der Aktivitäten gewährleistet ist. Alle Benutzer, einschliesslich der Supervisoren, unterliegen denselben Anmeldemechanismen und Passwortanforderungen.
- **Sitzungsverwaltung**: Nach der Authentifizierung wird ein **JWT-Token** ausgegeben, um den Zugriff auf die Funktionen der Anwendung auf der Grundlage der für jeden User konfigurierten Zugriffsrolle zu regeln. Die JWT-Einrichtung minimiert Risiken wie Session Hijacking und unbefugten Zugriff.
- **Zusätzliche Sicherheit:** Die Token sind so konfiguriert, dass sie nach bestimmten Intervallen ablaufen, was die Auswirkungen eines möglichen Token-Diebstahls verringert.

3.2 Zugriff auf das AWS-System (insbesondere AWS-SES)

- Wir verwenden AWS SES ausschliesslich für den Versand von Emails. Zugriff haben einzig atwork Entwickler.
- Das für SES verwendete AWS-Konto entspricht dem AWS-Root-Konto. Der Zugriff auf dieses Konto wird durch die standardmässige AWS-Passwortrichtlinie (mindestens 8 Zeichen, einschliesslich der von AWS definierten Komplexitätsanforderungen) in Kombination mit der obligatorischen Multi-Faktor-Authentifizierung (MFA) geschützt. Die MFA wird durch eine Authentifizierungsanwendung durchgesetzt, die zeitbasierte Einmalcodes generiert, die für jede Anmeldung erforderlich sind.
- Dieses Stammkonto verfügt über vollständige Administratorrechte innerhalb von AWS, wird in der Praxis jedoch nur für die Konfiguration und Wartung des SES-Dienstes verwendet. Eine begrenzte Anzahl von atwork-Entwicklern und Verwaltungsmitarbeitern hat Zugriff auf die Anmeldedaten. Die Anmeldedaten (Benutzername und Passwort) werden unter den autorisierten Personen geteilt, und der Zugriff wird widerrufen, wenn er nicht mehr benötigt wird, indem das Kontopasswort geändert wird.

- Das Konto wird intern von atwork verwaltet. In AWS sind keine zusätzlichen IAM-Benutzer konfiguriert, und alle Berechtigungen sind direkt mit dem Root-Konto verknüpft.
- Der Zugriff auf AWS erfolgt über die AWS-Webschnittstelle unter Verwendung dieses gemeinsamen Kontos. Für diesen AWS-Benutzer ist die Multi-Faktor-Authentifizierung aktiviert.
- Der AWS-Benutzer verfügt über vollständige Administratorrechte innerhalb des AWS-Kontos in Bezug auf SES.

3.3 Zugriff auf das Azure OpenAI-System

- Der Zugriff auf die Azure OpenAI-Ressourcen ist auf die erforderlichen Mitarbeiter unseres Unternehmens beschränkt, die für die Konfiguration und Wartung verantwortlich sind.
- Die Zugriffsverwaltung erfolgt über das rollenbasierte Zugriffskontrollsystem (RBAC) von Azure. Unsere Anwendung greift über denselben kontrollierten Mechanismus auf den Dienst zu.
- Den Benutzern werden gemäss dem Prinzip der geringsten Berechtigungen nur die für die Erfüllung ihrer Aufgaben erforderlichen Mindestrollen zugewiesen.
- Der Zugriff auf den Azure OpenAI-Dienst erfolgt nicht über API-Schlüssel, sondern ausschliesslich über das Benutzer- und Berechtigungsmanagementsystem von Azure.

4 User Flow

4.1 User-Onboarding

Bevor Mitarbeitende des Kunden X Zugang zu den Diensten bekommen, richtet atwork ein Admin-Profil ein (s. "Zugangsrollen"). Der Admin kann dann User hinzufügen, indem er die Informationen im User Profil eingibt. User können unvollständige Informationen ergänzen, sobald sie auf ihr Konto zugreifen, indem sie die fehlenden Fields ausfüllen. Der Admin kann jedem User jederzeit die Admin-Rolle zuweisen, so dass dieser auch zum Admin wird. Der Admin mit weiterreichendem Zugriff als der User kann sein Konto zudem auch wie ein User verwenden.

User erhalten einen individuellen Link per E-Mail (s. auch "Verschlüsselung und Datenschutz"), mit dem sie ein Konto einrichten können. Sie klicken den Link an und legt ein Passwort fest, mit dem sie jederzeit auf die Anwendung zugreifen können. Der Kunde Xist dafür verantwortlich, dass die User ihre Anmeldedaten nicht weitergeben. Atwork bietet auf Anfrage Schulungen zu diesem und ähnlichen Sicherheitskonzepten an. Die User melden sich über die folgende URL bei der atwork-Webanwendung an: https://kunde.atwork.ai/. Die User stellen die Verbindung zur Anwendung über den Standard-Port 443 her.

4.2 Zugang zu Umfragen

In der Anwendung können User auf Umfragen zugreifen. Die Umfragen bestehen aus vorkonfigurierten Umfragen, die atwork standardmässig zur Verfügung stellt, und zusätzlichen Umfragen, die von Admins erstellt werden können. Ein Admin muss Umfragen veröffentlichen, damit die User sie sehen können. Der User kann jederzeit wählen, ob seine Eingaben anonym sein sollen oder nicht. Der Default-Mode ist anonym. Um die ausgefüllte Umfrage nach dem Absenden für den User zugänglich zu machen, verwendet atwork eine *ID*, die die Umfrage mit dem User verknüpft. Niemand in der Organisation hat Zugriff auf die *ID*. Nur atwork-Entwickler haben Zugriff. Dieser Zugang wird nicht mit dem Kunde X geteilt.

Zugang zu Umfragen:

- Admins haben Zugriff auf den Umfragenersteller, können Umfragen für User freigeben und haben Zugriff auf alle eingereichten Antworten. Diese Antworten können nur dann mit dem jeweiligen User verknüpft werden, wenn dieser der Freigabe seines Namens zustimmt.

Der Zugang der User ist auf die ihnen von den Admins zur Verfügung gestellten Umfragen und ihre eigenen Antworten beschränkt. Die Zugangsrollen werden weiter oben unter Zugangsrollen und im Anhang in den Tabellen 1-3 genauer beschrieben.

4.3 Umfragen

Die Felder der Umfrage können durch Admins individuell angepasst werden. Die folgenden Angaben sind daher nur Beispiele. Die Logik der Dienste funktioniert so, ass Umfragen über das Feld *ID Tag* ("Key") mit den Userprofilen (siehe Tabelle 1) verknüpft werden. Dabei werden nur die markierten Felder abgerufen und angezeigt. Andere Felder sind entweder basierend auf der Zugangsrolle oder vollständig vom Zugang durch Kunden-Mitarbeitende ausgeschlossen und werden durch die Einschränkungen der Datenbanksuchanfragen nicht abgerufen. Die Zusammenführung der beiden Datenbanken wird in den Tabellen 2 und 3 im Anhang durch graue Schattierung dargestellt. Diese werden in der Logik der Dienste separat betrachtet und basierend auf Anfragen dynamisch zusammengeführt.

Zusätzlicher Hinweis: Theoretisch könnten Admins Umfragefelder mit einem PII Field wie Name oder Adresse festlegen, was wiederum zum Sammeln und verfügbarmachen von PII Values führen könnte. Hier gilt es, die Admins in der Erstellung der Umfragen zu schulen und interne Regeln zu erstellen (z.B. "Das Erstellen von Fields, die auf PII abzielen, ist nicht gestattet. Bitte beachtet das bei der Erstellung von Umfragen") und User bei der Nutzung zu informieren (z.B. "Bitte gebt PII nur in euren Userprofilen an, aber niemals in Textfelder von Umfragen")

5 Detailbeschreibung Integration Azure OpenAI Service

5.1 Allgemeines

Als Default-LLM-Provider für Natural Language Processing nutzt atwork Azure OpenAI Service.

Die Default-Lösung ist so strukturiert, dass grundsätzlich keine Inhalte der designierten PII-Fields an die Azure OpenAI Service gesendet werden. Eine genaue Übersicht der Fields, deren Inhalte an Azure OpenAI Service gesendet werden, kann den Tabellen 1-3 (s. Anhang) entnommen werden.

Bei denjenigen Inhalten, welche an Azure OpenAI Service gesendet werden, sorgt zusätzlich die Funktion für persönlich identifizierbare Informationen (PII) innerhalb der Azure AI Services for Language dafür, dass sensible Informationen und personenbezogene Daten, die in Test Fields landen, pseudonymisiert respektive unkenntlich gemacht werden.

Das Risiko das PII die Azure Umgebung verlassen kann ist sehr stark eingeschränkt. Ausserdem schränken zusätzliche Sicherheitsschichten und Mitarbeiterschulungen das Risiko weiter ein.

Vertraglich stellt atwork zudem sicher, dass:

- Microsoft keine Inhalte von atwork zu Trainingszwecken speichert.
- Userdaten von atwork nicht für das KI-Training verwendet werden.
- bei der API-Nutzung die Eingaben nur so lange gespeichert werden, wie dies für die Bereitstellung des Dienstes erforderlich ist.
- die Azure OpenAI-Ressource in der Region Schweiz Nord bereitgestellt wird. Aufgrund aktueller Dienstbeschränkungen in Schweizer Regionen wird die Datenverarbeitung jedoch über die von Azure OpenAI bereitgestellte globale Standardkonfiguration abgewickelt.
- alle an den Dienst gesendeten Daten werden vor der Übertragung anonymisiert werden.

Die von atwork verwendete Azure OpenAI-Ressource wird in der Region Schweiz Nord bereitgestellt. Aufgrund der aktuellen Servicebeschränkungen von Azure OpenAI erfolgt die Verarbeitung der Daten jedoch über die globale Standardbereitstellung von Microsoft, die auf der globalen Infrastruktur von Microsoft ausgeführt wird. Das bedeutet, dass Daten in Regionen ausserhalb Europas, einschliesslich der Vereinigten Staaten, verarbeitet werden können.

Was die Datenspeicherung betrifft, so können Anfragen und Antworten zu betrieblichen Zwecken, wie Überwachung, Diagnose und Nutzungsmetriken, vorübergehend in den

Systemen von Microsoft gespeichert werden. Diese Daten werden nicht für das Modelltraining verwendet, und die Speicherung ist vorübergehend und wird von Microsoft gemäss seinen internen Richtlinien verwaltet. Im Rahmen unseres Azure OpenAI-Abonnements werden Eingabeaufforderungen und Antworten nicht für das Modell-Retraining gespeichert, und wir führen keine dauerhaften Protokolle über die Nutzung von Kundenanfragen.

Um das Risiko einer Offenlegung personenbezogener Daten zu minimieren, wendet unsere Anwendung eine Anonymisierung für automatisierte Datenflüsse an. Für Flüsse, die auf direkte Benutzeranfragen reagieren, wird keine Anonymisierung angewendet, da die übertragenen Daten dies nicht erfordern.

Diese Konfiguration spiegelt die aktuellen technischen Einschränkungen von Microsoft wider, das noch keine vollständig regionalisierte Bereitstellung von Azure OpenAI in der Schweiz anbietet.

Alle an Azure OpenAI übertragenen Daten werden sicher über HTTPS (TLS) verarbeitet, und es werden die standardmässigen Azure-Sicherheits- und Zugriffskontrollen angewendet, um den Zugriff auf autorisiertes Personal zu beschränken.

5.2 Zugriffsverwaltung und Sicherheit

Wir verwenden standardmässige, bewährte Azure-Mechanismen, um eine sichere Integration mit dem Azure OpenAI-Dienst zu gewährleisten. Unsere Anwendung greift über eine vom System zugewiesene Azure Managed Identity mit eingeschränkter Rolle auf den Azure OpenAI-Endpunkt zu, sodass keine API-Schlüssel oder Geheimnisse erforderlich sind. Die gesamte Kommunikation mit dem Azure OpenAI-Endpunkt erfolgt über HTTPS (TLS) unter Verwendung des offiziellen .NET Azure.AI.OpenAI SDK, das standardmässig eine verschlüsselte Übertragung gewährleistet.

Obwohl wir in unserer aktuellen Konfiguration keine dedizierte Webanwendungs-Firewall (WAF) oder virtuelle Netzwerktrennung verwenden, ist der Zugriff auf die Azure-Ressourcen streng auf autorisiertes Personal zu Konfigurations- und Wartungszwecken beschränkt. Protokolle und Überwachung sind über die standardmässigen Telemetrie- und Diagnosefunktionen von Azure verfügbar.

Weitere Informationen zu den von Azure OpenAI Service angewandten Best Practices für Sicherheit und Zugriffsverwaltung finden Sie in der offiziellen Dokumentation: https://learn.microsoft.com/en-us/azure/ai-foundry/responsible-ai/openai/data-privacy?tabs=azure-portal

5.3 Nutzungsszenarien Azure OpenAI Service

Datenverarbeitung: Azure OpenAI Service wird in den folgenden zwei spezifischen Szenarien verwendet:

Szenario 1: Aggregierte Datenanalyse basierend auf quantitativen Daten: Azure OpenAI Service wird verwendet, um Verbesserungen basierend auf aggregierten Daten vorzuschlagen. Admins sehen im Dashboard eine Übersicht der aggregierten Daten und können somit Problemfelder identifizieren, z.B "Durchschnittliche Zufriedenheit: 4". Nun können sie entscheiden, dass die Zufriedenheit erhöht werden soll und über Azure OpenAI Service Handlungsoptionen generieren lassen. Hierbei wird folgendes an die API gesendet: "Field (ohne Inhalt ("Value"))". Im Beispiel würde als nur "Durchschnittliche Zufriedenheit" gemeinsam mit einem vordefinierten System Prompt der auf Handlungsoptionen abzielt an Azure OpenAI Service gesendet. Der Systemprompt enthält auch das Unternehmensprofil. Dieses kann von jedem Admin erstellt werden z.B. Unsere Organisation ist ein mittelgrosses Krankenhaus.

Potenzielles Risiko: Admin fügt PII in die Unternehmensbeschreibung ein. Beispiel: Unser Unternehmen heisst Kunde X und Hans Meier arbeitet bei uns.

Massnahme: Selbstorganisierte Mitarbeiter-Schulung. Begrenzung der Admins auf geschulte Mitarbeiter. atwork kann auf Anfrage eine Mitarbeiterschulung anbieten.

Szenario 2 Aggregierte Datenanalyse basierend auf qualitativen Daten: Azure OpenAI Service wird verwendet, um die Kommentare und andere Textinputs der User in den Umfragen zu bündeln und eine aggregierte Analyse und Handlungsoptionen in Form von Text zu generieren. Beispiel: **User Eingaben (Input Azure OpenAI Service):** "Ich verliere jeden Tag viel Zeit beim Mittagessen, weil die Schlangen in der Cafeteria so lang sind.", "Die Wartezeiten in der Cafeteria sind zu lang. Das Mittagessen dauert viel länger als nötig.", "Es wäre hilfreich, wenn die Cafeteria effizienter organisiert wäre, um die langen Schlangen zu vermeiden.", "Ich finde es frustrierend, dass ich so viel Zeit in der Schlange verbringen muss, anstatt meine Mittagspause zu geniessen.", "Die langen Schlangen in der Cafeteria führen dazu, dass ich weniger Zeit habe, um mich zu entspannen und mein Mittagessen zu geniessen. "**Analyse (Output von Azure OpenAI Service):** Viele Mitarbeiter der Organisation verlieren Zeit aufgrund langer Wartzeiten in der Mittagspause. **Handlungsoption (Output von Azure OpenAI Service):** Führen Sie wenn möglich gestaffelte Mittagszeiten ein. Hierbei werden die Field Bezeichnungen, Texteingaben als Value und ein Systemprompt inklusive Unternehmensprofil an Azure OpenAI Service gesendet. Z.B. **User Inputs: Field:** Zeitmanagement: **Values:** [Siehe Beispiele unter **Eingaben (Input Azure OpenAI Service):**]. + **Systemprompt:** Basierend auf der Unternehmensbezeichnung und den beigefügten Themen inklusive Kommentare dazu identifiziere mögliche Handlungsfelder + **Unternehmensprofil:** Unsere Organisation ist ein mittelgrosses Krankenhaus.

Potenzielles Risiko: Admin fügt PII in die Unternehmensbeschreibung ein, z.B. "Unser Unternehmen heisst Kunde X und Hans Meier arbeitet bei uns". User fügt PII in ein Textfeld ein z.B. "Ich verliere viel Zeit weil mein Vorgesetzter bei der Kunde X Hans Meier immer so langsam isst und ich nicht unhöflich sein möchte".

Massnahme: Atwork hat hier einen zusätzlichen Sicherheitsmechanismus eingesetzt. Mittels Azure AI Language PII Detection wird PII in den Texteingaben identifiziert und entfernt. Das

ersetzt aber nicht folgende Präventionsmechanismen: Selbstorganisierte Mitarbeiter-Schulung. Begrenzung der Admins auf geschulte Mitarbeiter. Atwork kann auf Anfrage eine Mitarbeiterschulung anbieten.

Einschränkungen: Azure OpenAI Service erhält nur die genannten Dateneingaben, insbesondere werden keine persönlich identifizierenden Fields ("PII Fields") wie *First Name, Last Name und E-Mail* an Azure OpenAI Service gesendet.

Sicherheitsmassnahmen:

- **Azure AI Language PII Detection:** Diese Funktion entfernt persönlich identifizierbare Informationen aus Textdaten, bevor sie an Azure OpenAI Service gesendet werden.
- **Anonymisierung:** Daten werden anonymisiert, indem Texteingaben aggregiert als API Anfrage gesendet werden und in dem PII Fields nicht an die API gesendet werden.
- **Protokollierung und Überwachung:** Alle Datenübertragungen und -verarbeitungen werden protokolliert ("Log") und können überprüft werden, um die Einhaltung der Datenschutzrichtlinien sicherzustellen.

5.4 Beschreibung Datenfluss Azure OpenAI Service inkl. Screenshots

Wir senden Daten wie oben beschrieben an Azure OpenAI Service, um die Funktionalität zu verbessern. Im Folgenden finden Sie eine Aufschlüsselung, was wann gesendet wird:

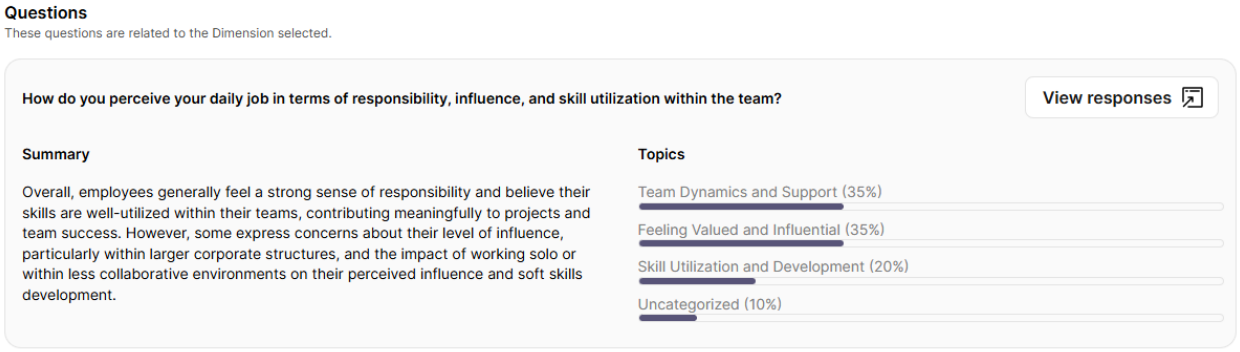
Anonymisierte qualitative Textanalysen:

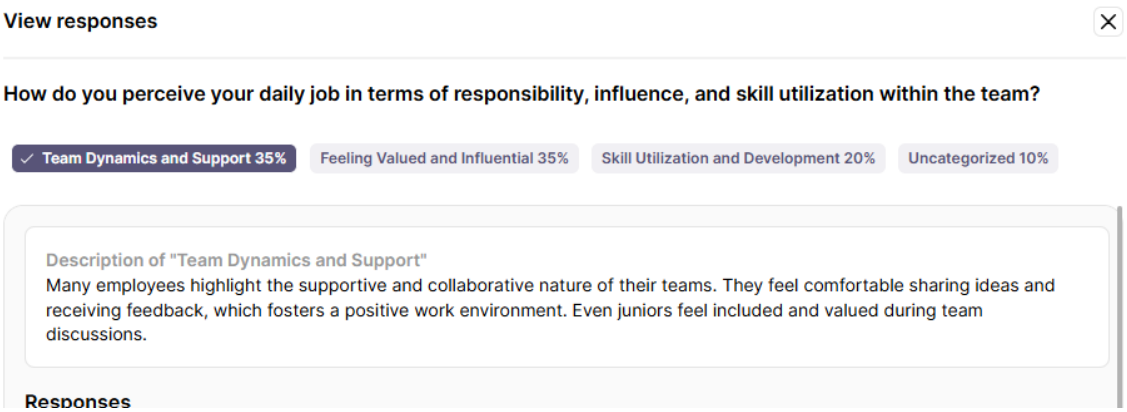
Wenn eine Umfrage offene Textfragen enthält, werden die Antworten (ohne personenbezogene Daten, wie oben beschrieben) nach Abschluss der Umfrage an Azure OpenAI Service zur Verarbeitung ("natural language processing") gesendet.

Azure OpenAI Service analysiert die anonymisierten Antworten um

- Zusammenfassungen zu erstellen,
- Themen zu identifizieren,
- und Kommentare zu klassifizieren.

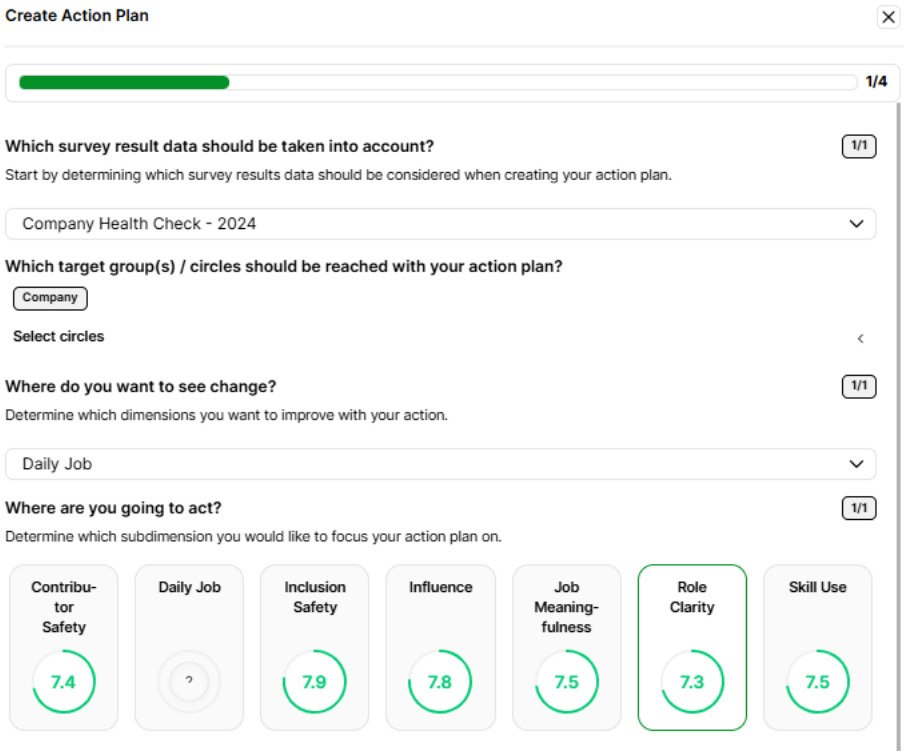
Nachstehend finden Sie ein Beispiel eines Screenshots direkt von atwork:



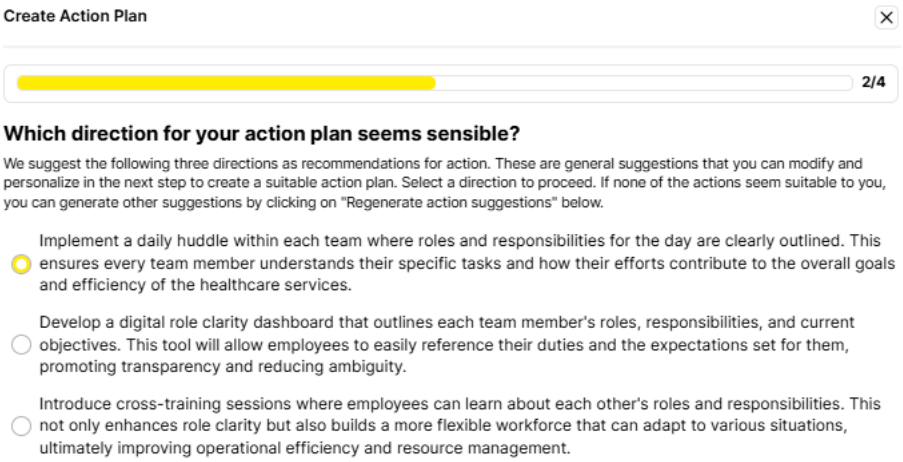


Handlungsempfehlungen: Auf Wunsch des Users können wir den Usern gestützt auf die Umfrageergebnisse Handlungsempfehlungen in Form von Aktionsplänen zur Verfügung stellen. Um den Usern Aktionspläne zur Verfügung zu stellen, werden die Daten wie folgt mit Azure OpenAI Service ausgetauscht:

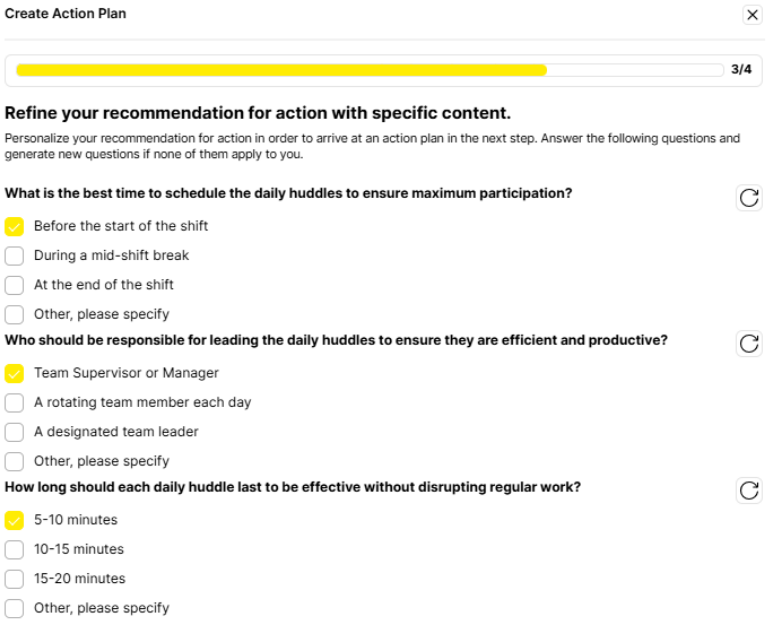
- Es werden keine qualitativen oder quantitativen Umfrageergebnisse veröffentlicht. Stattdessen teilen wir:
    - **Phase 1:** Wir versenden ausgewählte "Handlungsfelder" (z.B. Rollenklarheit), "Dimensionen" (z.B. tägliche Arbeit) und ein vom Admin definiertes "Unternehmensprofil". Nur das Profil (z.B. Abteilung X mit 200 Mitarbeitenden) wird an Azure OpenAI Service weitergegeben; konkret bedeutet dies, dass Verweise auf das Kunde X vor der Weitergabe redigiert werden. Nachstehend finden Sie ein Beispiel eines Screenshots direkt von atwork mit Beispielergebnissen:



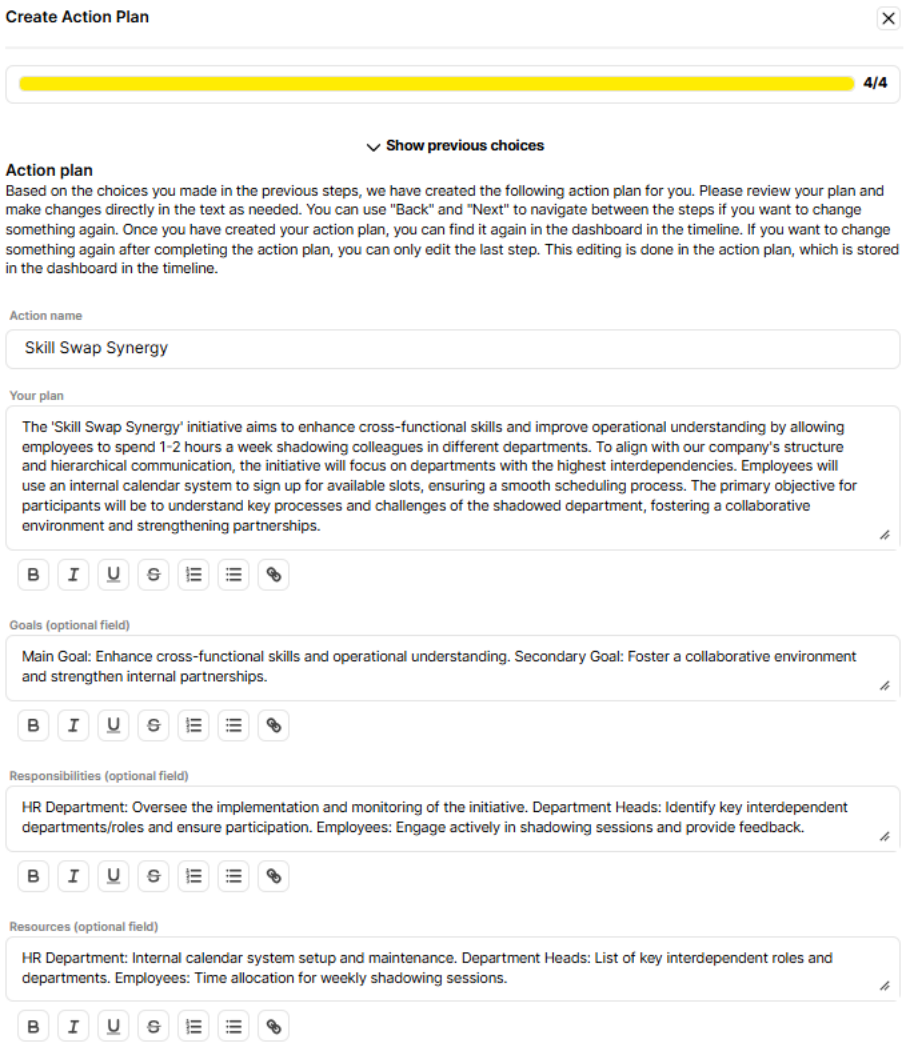
- **Phase 2:** Eine Auswahl erster Empfehlungen möglicher Aktionspläne wird von Azure OpenAI Service auf der Grundlage der bereitgestellten Informationen vorgeschlagen. Der User wählt aus, welcher Aktionsplan entwickelt und konkretisiert werden soll. Diese Auswahl wird mit Azure OpenAI Service geteilt. Nachfolgend finden Sie ein Beispiel eines Screenshots direkt aus atwork mit Beispielergebnissen:



- **Phase 3:** Dem User wird eine Reihe von zusätzlichen Fragen mit Multiple-Choice-Antworten gestellt. Die Multiple-Choice-Auswahl des Users wird mit Azure OpenAI Service geteilt.

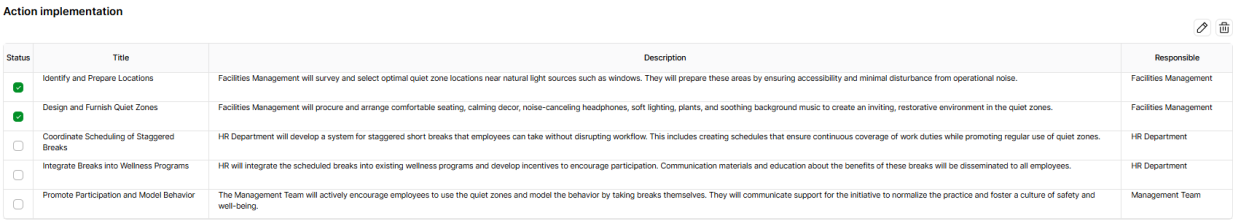


- **Phase 4:** Mit Hilfe von Azure OpenAI Service wird ein Entwurf für einen Aktionsplan erstellt, der den zusammengefassten Plan, die Ziele, die Verantwortlichkeiten und die benötigten Ressourcen enthält. Der Output von Azure OpenAI Service wird von den atwork-Mitarbeitern nicht mehr bearbeitet. Nachstehend finden Sie ein Beispiel eines Screenshots direkt von atwork mit Beispielergebnissen:



Umsetzung der Aktion: Wenn der Admin konkrete Schritte zur Umsetzung der Aktion auf der Grundlage des zuvor erstellten Aktionsplans wünscht, wird der Aktionsplan mit Azure OpenAI Service geteilt, um Umsetzungsschritte zu erstellen. Dazu gehören *Your plan*, *Goals (optional field), Responsibilities (optional field)* und *Ressources (optional field)*. Nachfolgend finden Sie ein Beispiel eines Screenshots direkt von atwork mit Beispielergebnissen, die von Azure OpenAI Service auf der Grundlage der anonymisierten Eingabedaten bereitgestellt werden.

Um Missverständnisse zu vermeiden: Die Organisationsstruktur des Unternehmens wird nicht mit Azure OpenAI Service geteilt, Struktur und Rollen sind Platzhalter, die von dem probabilistischen KI-Modell aus dem bereitgestellten Kontext abgeleitet werden:



Action implementation

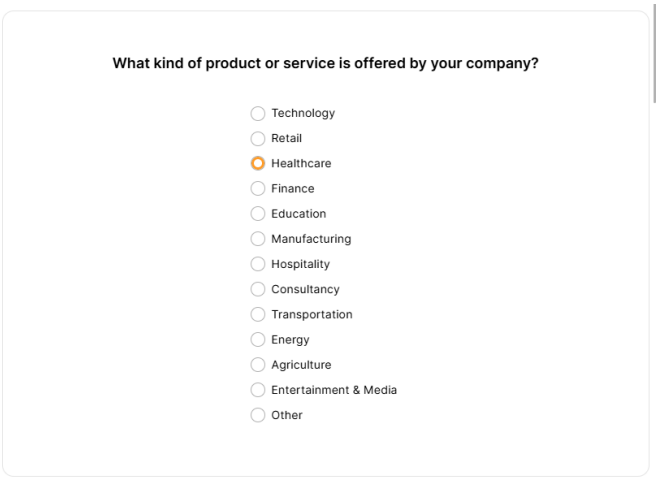
Status	Title	Description	Responsible
☑	Identify and Prepare Locations	Facilities Management will survey and select optimal quiet zone locations near natural light sources such as windows. They will prepare these areas by ensuring accessibility and minimal disturbance from operational noise.	Facilities Management
☑	Design and Furnish Quiet Zones	Facilities Management will procure and arrange comfortable seating, calming decor, noise-canceling headphones, soft lighting, plants, and soothing background music to create an inviting, restorative environment in the quiet zones.	Facilities Management
☐	Coordinate Scheduling of Staggered Breaks	HR Department will develop a system for staggered short breaks that employees can take without disrupting workflow. This includes creating schedules that ensure continuous coverage of work duties while promoting regular use of quiet zones.	HR Department
☐	Integrate Breaks into Wellness Programs	HR will integrate the scheduled breaks into existing wellness programs and develop incentives to encourage participation. Communication materials and education about the benefits of these breaks will be disseminated to all employees.	HR Department
☐	Promote Participation and Model Behavior	The Management Team will actively encourage employees to use the quiet zones and model the behavior by taking breaks themselves. They will communicate support for the initiative to normalize the practice and foster a culture of safety and well-being.	Management Team

Unternehmensprofil:

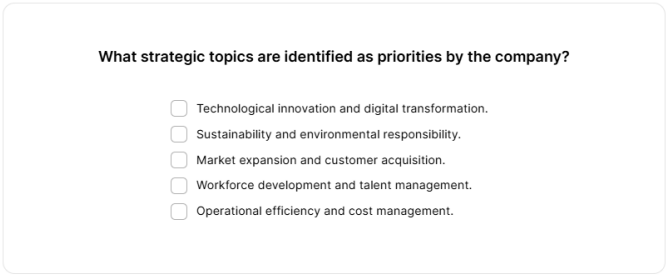
Die Admins von Kunde X können ein sogenanntes "Unternehmensprofil" für ihr Unternehmen erstellen und es mit Azure OpenAI Service als Teil des Prozesses zum Erhalt von Handlungsempfehlungen teilen. Dies dient dazu, die Qualität und Tiefe der bereitgestellten Handlungsempfehlungen zu verbessern. Das erstellte Unternehmensprofil gibt den Handlungsempfehlungen zusätzlichen organisatorischen Kontext.

Wenn ein Admin ein Unternehmensprofil seines Unternehmens in atwork erfasst, wird die Azure OpenAI Service für die Generierung einer Zusammenfassung (das eigentliche Unternehmensprofil) genutzt. Dieses Profil wird von Azure OpenAI Service auf der Basis der Antworten auf die folgenden Fragen von atwork erstellt. Im Folgenden finden Sie auch Screenshots mit Musterantworten:

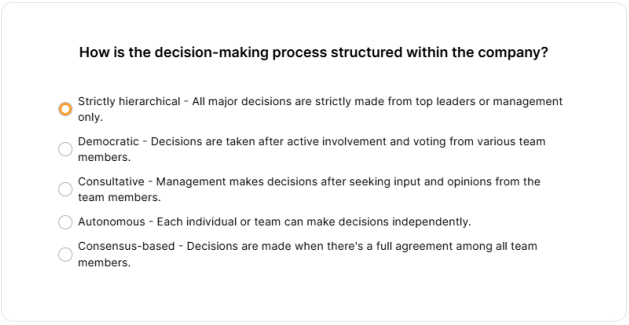
- *In welchem Land sind Sie ansässig?*
  - *(Dropdown)*
- *Welche Art von Produkt oder Dienstleistung wird von Ihrem Unternehmen angeboten?*



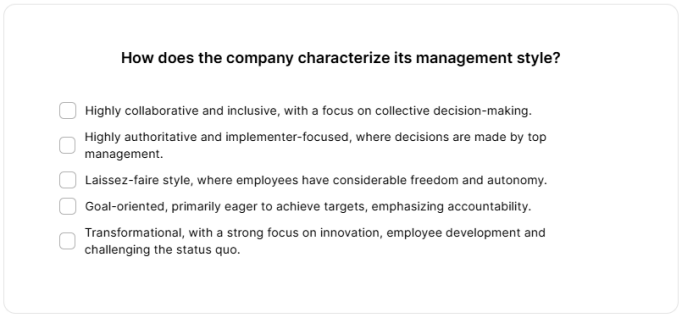
- *Welche strategischen Themen werden als vorrangig eingestuft?*



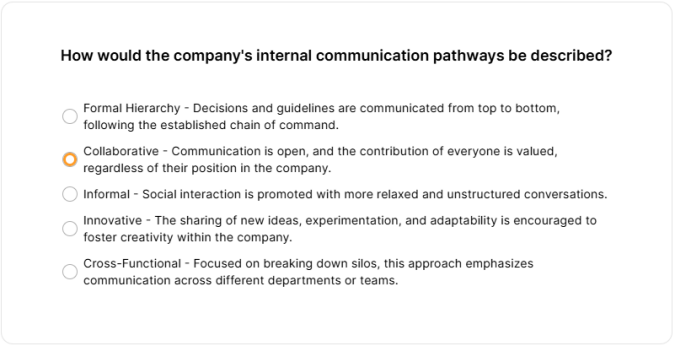
- *Wie ist der Entscheidungsfindungsprozess im Unternehmen strukturiert?*



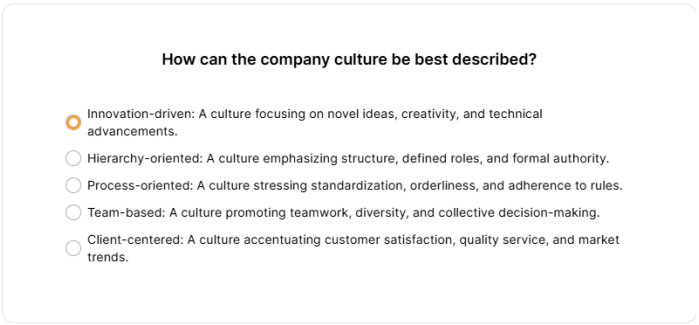
- *Wie charakterisiert das Unternehmen seinen Führungsstil?*



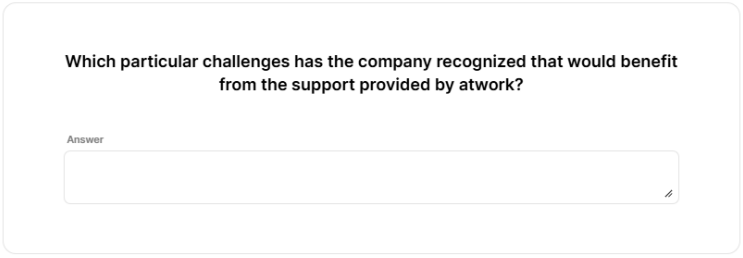
- *Wie würden Sie die internen Kommunikationswege des Unternehmens beschreiben?*



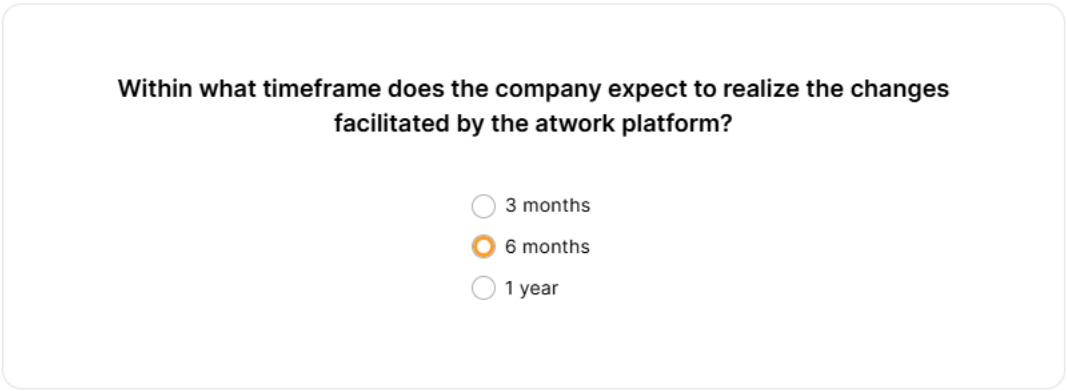
- *Wie lässt sich die Unternehmenskultur am besten beschreiben?*



- *Welche besonderen Herausforderungen hat das Unternehmen erkannt, die von der Unterstützung durch atwork profitieren würden?*



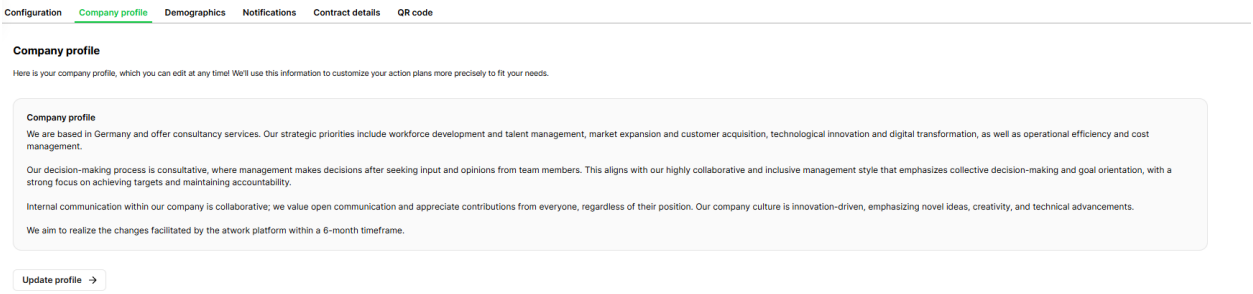
- *In welchem Zeitrahmen erwartet das Unternehmen, die durch die atwork-Plattform ermöglichten Veränderungen zu realisieren?*



- *Bitte geben Sie bei Bedarf weitere Informationen über Ihr Unternehmen an, die Sie für wichtig halten.*
    - *(offener Text)*

Wenn der Admin seine Antworten auf die gestellten Fragen ändert, werden die Korrekturen erneut an Azure OpenAI Service gesendet und der Prozess wird erneut durchgeführt, um das Unternehmensprofil entsprechend neu zu erstellen.

Hier ist ein Beispiel für die Antwort, die Azure OpenAI Service nach der Beantwortung der obigen Fragen gibt



6 Anhang: Datenbank und Zugriffsrechte im Überblick

6.1 Tabelle 1: User Profil

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
ID Tag	345234634	❌	❌	❌	❌
First Name	John	✅	❌	✅	❌
Last Name	Doe	✅	❌	✅	❌
Email Address	john.doe@example.com	✅	❌	✅	❌
Language	German	✅	❌	✅	❌
Kreise (with Subkreise)	{ "Company": { "Product": { "Design": null, "Development": null }, "Sales": {	✅	❌	✅	❌

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service

	"Sales Austria": null,
	"Sales Germany": {
	"Account Manager": null,
	"Interns": null
	}
	}
	}
	}				

Onboarding E-Mail	Yes	✅	❌	✅	❌
Gender	Male	✅	❌	✅	❌
Organisatorische Hierarchie	Management	✅	❌	✅	❌
Position	Product Owner	✅	❌	✅	❌
Beschäftigungsart	Part time	✅	❌	✅	❌
Arbeitsmodalitäten	Hybrid	✅	❌	✅	❌
Standort	Zürich	✅	❌	✅	❌
Age	26	✅	❌	✅	❌
Seniority (in years)	5	✅	❌	✅	❌

6.2 Tabelle 2: Umfrage Default-Mode

Hinweis

- Schattierung in grau: Die graue Schattierung in untenstehender Tabelle stellt die Zusammenführung beider Datenbanken dar. Diese werden in der Logik der Dienste separat betrachtet und und basierend auf Anfragen dynamisch zusammengeführt.

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
ID Tag	345234634	❌	❌	❌	❌
First Name	John	✅	❌	❌	❌
Last Name	Doe	✅	❌	❌	❌
Email Address	john.doe@example.com	✅	❌	❌	❌
Language	German	✅	❌	❌	❌
Kreise (with Subkreise)	{ "Company": { "Product": { "Design": null, "Development": null }, "Sales": { "Sales Austria": null, "Sales Germany": { "Account Manager": null, "Interns": null } } } }	✅	❌	Nur so detailliert, dass die Auswahl mindestens 5 ("Treshhold") Personen mit der gleichen Konfiguration enthält. Der Treshhold kann auf Anfrage erhöht werden.	❌
Onboarding E-Mail	Yes	✅	❌	❌	❌

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
Gender	Male	✅	❌	❌	❌
Organisatorische Hierarchie	Management	✅	❌	❌	❌
Position	Product Owner	✅	❌	❌	❌
Beschäftigungsart	Part time	✅	❌	❌	❌
Arbeitsmodalitäten	Hybrid	✅	❌	❌	❌
Standort	Zürich	✅	❌	❌	❌
Age	26	✅	❌	❌	❌
Seniority (in years)	5	✅	❌	❌	❌
ID Tag	345234634	❌	❌	❌	❌
Opt-In	false	✅	❌	❌	❌

Umfrage	"survey_responses": {
	"quantitative": {
	"overall_wellbeing": 8,
	"job_satisfaction": 7,
	"work_life_balance": 6,
	"manager_support": 9,
	"career_growth": 7
	},
	"qualitative": [
		✅	❌	✅	✅

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
	"Ich verliere jeden Tag viel Zeit beim Mittagessen, weil die Schlangen in der Kafeteria so lang sind.", "Die Wartezeiten in der Kafeteria sind zu lang. Das Mittagessen dauert viel länger als nötig.", "Es wäre hilfreich, wenn die Kafeteria effizienter organisiert wäre, um die langen Schlangen zu vermeiden.", "Ich finde es frustrierend, dass ich so viel Zeit in der Schlange verbringen muss, anstatt meine Mittagspause zu geniessen.", "Die langen Schlangen in der Cafeteria führen dazu, dass ich weniger Zeit habe, um mich zu entspannen und mein Mittagessen zu geniessen."				

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
	] }, "survey_date": "2025-03-25T10:59:02Z" }				

6.3 Tabelle 3: Umfrage Opt-In

Hinweis

- Schattierung in grau: Die graue Schattierung in untenstehender Tabelle stellt die Zusammenführung beider Datenbanken dar. Diese werden in der Logik der Dienste separat betrachtet und und basierend auf Anfragen dynamisch zusammengeführt.

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
ID Tag	345234634	❌	❌	❌	❌
First Name	John	✅	❌	✅	❌
Last Name	Doe	✅	❌	✅	❌
Email Address	john.doe@example.com	✅	❌	Kann durch Abfrage des User Profils identifiziert werden.	❌

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
Language	German	✅	❌	""	❌
Kreise (with Subkreise)	{ "Company": { "Product": { "Design": null, "Development": null }, "Sales": { "Sales Austria": null, "Sales Germany": { "Account Manager": null, "Interns": null } } } }	✅	❌	Nur so detailliert, dass die Auswahl mindestens 5 ("Treshhold") Personen mit der gleichen Konfiguration enthält. Der Treshhold kann auf Anfrage erhöht werden.	❌
Onboarding E-Mail	Yes	✅	❌	Kann durch Abfrage des User Profils identifiziert werden.	❌
Gender	Male	✅	❌	""	❌

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
Organisatorische Hierarchie	Management	✅	❌	""	❌
Position	Product Owner	✅	❌	""	❌
Beschäftigungsart	Part time	✅	❌	""	❌
Arbeitsmodalitäten	Hybrid	✅	❌	""	❌
Standort	Zürich	✅	❌	""	❌
Age	26	✅	❌	""	❌
Seniority (in years)	5	✅	❌	""	❌
ID Tag	345234634	❌	❌	❌	❌
Opt-In	true	✅	❌	❌	❌

Umfrage	"survey_responses": {
	"quantitative": {
	"overall_wellbeing": 8,
	"job_satisfaction": 7,
	"work_life_balance": 6,
	"manager_support": 9,
	"career_growth": 7
	},
	"qualitative": [
	"Ich verliere jeden Tag viel Zeit beim
		✅	❌	✅	✅

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
	Mittagessen, weil die Schlangen in der Cafeteria so lang sind.", "Die Wartezeiten in der Cafeteria sind zu lang. Das Mittagessen dauert viel länger als nötig.", "Es wäre hilfreich, wenn die Cafeteria effizienter organisiert wäre, um die langen Schlangen zu vermeiden.", "Ich finde es frustrierend, dass ich so viel Zeit in der Schlange verbringen muss, anstatt meine Mittagspause zu geniessen.", "Die langen Schlangen in der Cafeteria führen dazu, dass ich weniger Zeit habe, um mich zu entspannen und mein Mittagessen zu geniessen."]				

Field	Value	User (eigenes Profil)	User (fremdes Profil)	Admin	Azure OpenAI Service
	}, "survey_date": "2025-03-25T10:59:02Z" }				