tellent

R:Tellent-Whitepaper
Sicherheit, Compliance und Betrieb

Mit diesem Dokument bietet Ihnen Tellent Transparenz und Klarheit über die Sicherheits-, Compliance- und Betriebsrichtlinien, die die Grundlage für unser Geschäft und unsere Partnerschaften bilden. Denn wir wissen, dass die Beauftragung eines Dienstleisters eine wichtige unternehmerische Entscheidung ist, die – wie jede Partnerschaft – auf Vertrauen basieren sollte.

Dieses Dokument gibt einen allgemeinen Überblick über die Sicherheitsmaßnahmen von Tellent als Unternehmen und in den Software-as-a-Service-Produkten/Modulen von Tellent:

- KiwiHR von Tellent, ein zentrales Personalverwaltungssystem
- Javelo von Tellent, ein Performance-Management-System
- Recruitee von Tellent, ein Bewerber-Tracking-System
- Jeder andere Service, der eine konsistente Funktionalität zwischen den oben genannten Produkten/Modulen bietet.

Bei Fragen wenden Sie sich bitte an Tellent über den In-App-Support-Chat oder direkt an das Sicherheitsteam unter: security@tellent.com

tellent

Inhaltsverzeichnis

tellent

Compliance, Zertifizierungen und Auditberichte

ISO 27001-Zertifizierung und SOC-2-Zertifizierungsbericht

Tellent:

- ISO 27001:2022
  - Eine Kopie der ISO-27001-Zertifizierung von Tellent finden Sie hier.
  - Die ISO-27001-Anwendbarkeitserklärung von Tellent finden Sie hier.
  - Geltungsbereich der ISO-27001-Zertifizierung von Tellent: *Die sichere Entwicklung, der sichere Betrieb und die sichere Bereitstellung der folgenden Tellent-Software as a Service-Produkte/Module: Kerninformationssystem für das Personalwesen (auch unter dem Markennamen „KiwiHR“ vermarktet), Leistungsmanagement (auch unter dem Markennamen „Javelo“ vermarktet), Bewerber-Tracking-System (auch unter dem Markennamen „Recruitee“ vermarktet) und alle Produkte/Module, die gemeinsame Funktionen zwischen diesen Produkten/Modulen bereitstellen.*

Recruitee SaaS:

- SOC 2
  - Eine Kopie des SOC-2-Berichts (SSAE 16/ISAE 3402 Typ II) für Recruitee kann auf Anfrage zur Verfügung gestellt werden.

Interne Audits und Penetrationstests

- Der Informationssicherheitsbeauftragte (ISO) von Tellent überprüft zusammen mit verschiedenen spezialisierten externen Auditoren die Sicherheit der Dienste und Unternehmensprozesse.
- Penetrationstests werden regelmäßig von renommierten Sicherheitsunternehmen durchgeführt.
- Kunden können auf Anfrage eigene Penetrationstests und Audits durchführen.

DSGVO

- Tellent unterstützt Sie bei der Einhaltung der Datenschutz-Grundverordnung (DSGVO) mit speziellen DSGVO-Funktionen.
  - Unsere engagierten Customer-Success-Manager und unser Support-Team können Sie bei der Konfiguration unterstützen und alle Fragen zu den Funktionen beantworten.
- Unser Standard-Datenverarbeitungszusatz (Data Processing Addendum, DPA) ist Teil der Vereinbarung zwischen Tellent und Ihnen als Kunde, sofern nicht ausdrücklich etwas anderes vereinbart wurde.
- Die Einhaltung der DSGVO durch Tellent wird von der internen Rechtsabteilung von Tellent überwacht.
- Alle personenbezogenen Daten, die im Auftrag unserer Kunden verarbeitet werden, werden innerhalb der Europäischen Union gespeichert und ohne Ihre Zustimmung nicht an Drittländer weitergegeben.

- Tellent kommt Anfragen von Behörden nach Zugang zu (personenbezogenen) Daten nur in dem Umfang nach, in dem Tellent aufgrund geltender Gesetze und Vorschriften dazu verpflichtet ist.

Kundendaten (einschließlich personenbezogener Daten der Kunden)

- Kundendaten sind alle Daten, einschließlich personenbezogener Daten, die Tellent im Rahmen von SaaS im Namen des Kunden verarbeitet, mit Ausnahme von Backups.
- Insbesondere in Bezug auf die personenbezogenen Daten eines Kunden gilt der Kunde als Verantwortlicher für diese personenbezogenen Daten und Tellent als Datenverarbeiter, wie in unserem Standard-Datenverarbeitungszusatz (DPA) näher definiert.
- Tellent verkauft, bewirbt oder verwendet Kundendaten niemals auf eine andere Weise als zur Bereitstellung oder Verbesserung der Dienstleistungen für seine Kunden.
- Kunden können Kundendaten über die APIs von Tellent oder die als Teil des SaaS bereitgestellten Exportfunktionen exportieren.

Anwendungssicherheit

Identitäts- und rollenbasierter Zugang

Der Mitgliederstatus und der Zugang zu Rollen und Berechtigungen können im Tellent-Admin-Center und/oder individuell über Recruitee SaaS, Javelo SaaS oder KiwiHR SaaS definiert werden.

Durch diese verschiedenen Einstellungen ist es (zum Beispiel) möglich:

- in Recruitee SaaS die Informationen über offene Stellen auf Personalverantwortliche zu beschränken;
- in Javelo SaaS den Status oder die Ergebnisse offener Umfragen oder Kampagnen nur den Mitgliedern Ihres HR-Teams anzuzeigen;
- in KiwiHR SaaS direkten Vorgesetzten die Berechtigung zu geben, die Daten und Details eines Mitarbeiters einzusehen;
- in Recruitee SaaS Bewerberdaten über eindeutige Links mit Nicht-Benutzern zu teilen;
- in Recruitee SaaS Sichtbarkeitsfunktionen auf Profilfelder von Bewerbern anzuwenden, um z. B. Gehaltsinformationen vor der Ansicht zu schützen.

Einen Support-Artikel mit weiteren Informationen zur Verwaltung der Kontoeinstellungen im **Tellent-Admin-Center** finden Sie unter:
https://support.tellent.com/en/collections/9447061-account-settings

Einen Support-Artikel mit weiteren Informationen zur Verwaltung der Kontoeinstellungen in **Javelo SaaS** finden Sie unter:
https://support.javelo.com/en/collections/9545584-account-settings

Einen Support-Artikel mit weiteren Informationen zur Verwaltung der Benutzerrollen in **KiwiHR SaaS** finden Sie unter: https://support.kiwihr.com/en/articles/9345339-user-roles & https://support.kiwihr.com/en/articles/9345338-access-levels

Einen Support-Artikel mit weiteren Informationen zu Benutzerrollen (Personalverantwortliche) in **Recruitee SaaS** finden Sie unter: https://support.recruitee.com/en/articles/1066251-hiring-roles

Sicherheit der Datenübertragung und Verschlüsselung

- Alle Daten werden über das Internet mit TLS 1.2 oder höher mit einer Schlüssellänge von mindestens 2048 Bit übertragen.
- Cookies, die sensible Informationen enthalten, werden auf „sicher“ und „nur über http“ gesetzt.
- Kundendaten werden im Ruhezustand verschlüsselt (AES 256 oder höher).

Sichere Kodierung

- Die Bemühungen der Entwickler zielen darauf ab, die OWASP Top-10-Risiken zu minimieren und den Best Practices für Sicherheit in der Industrie zu folgen.
- Automatisierte Tests werden eingerichtet, um automatisch zu überprüfen, ob die Anwendung wie erwartet funktioniert.
- Automatisierte Tests werden eingerichtet, um automatisch nach Schwachstellen in Code und Abhängigkeiten zu suchen.
- Neuer Code wird vom Qualitätssicherungsteam von Tellent getestet.
- Produktionsdaten werden niemals zum Testen verwendet. Tellent hat (eine) separate Staging-Umgebung(en).
- Der gesamte Code wird einer Codeüberprüfung unterzogen.

Schutz gegen Malware und Cross-Site-Scripting

- Dateiuploads von Bewerbern und Endnutzern werden auf Malware geprüft. Definitionen werden automatisch und regelmäßig aktualisiert.
- Daten aus Benutzereingabefeldern werden bereinigt.
- Die Entwickler befolgen Best Practices wie die OWASP Top-10, um Cross Site Scripting (XSS), SQL Injection (SQLi) und Cross Site Request Forgery (CSRF) zu verhindern.

Authentifizierung

- Es ist möglich, einen eigenen Single Sign-On Identity Provider (über SAML 2.0) zu integrieren.
    - Für Konten ohne SSO basiert die Anmeldung auf der E-Mail-Adresse und dem Passwort des Endnutzers.
    - Neue Passwörter müssen mindestens 8 Zeichen lang sein und folgende Zeichen enthalten: Großbuchstaben, Kleinbuchstaben und Ziffern.
- Nach erfolgreicher Authentifizierung wird ein Zugriffstoken ausgegeben.
    - Jedes Endgerät erhält einen anderen, individuellen Zugriffstoken.

    - Die Token werden sicher gespeichert (Cookies, „sicher“ und „nur über http“).
- Alle Zugriffstoken werden widerrufen, wenn ein Benutzer sein Passwort ändert. Dies gilt auch für Passwortänderungen über die Funktion „Passwort vergessen“.
- Zugriffstoken verfallen nach 30 Tagen und werden widerrufen, wenn sich ein Endnutzer abmeldet. Alte Token werden regelmäßig durch neue ersetzt, wenn die Anwendung weiter genutzt wird.
- Tellent speichert nur Hashes von Benutzerkonto-Passwörtern, nicht die Passwörter selbst. Die Hashes werden mit einem starken Industriestandard-Algorithmus und in Übereinstimmung mit Best Practices generiert.
- Nach einer hohen Anzahl von Anmeldeversuchen für ein Konto wird dieses vorübergehend gesperrt.

E-Mail-Schutz

- Die Tellent-Server für ein- und ausgehende E-Mails unterstützen TLS.
- SPF, DMARC und DKIM werden für alle ausgehenden E-Mails verwendet.
- Der Kunde kann die Sicherheit der E-Mail-Integration vollständig kontrollieren, indem er Recruitee SaaS über TLS mit seinen eigenen IMAP- und SMTP-Servern verbindet. Dadurch profitiert der Kunde auch von SPF, DKIM und DMARC.
- Recruitee SaaS bietet auch die Möglichkeit, Bewerber über HTTPS statt über weniger sichere E-Mail-Protokolle an Nicht-Benutzer weiterzuleiten.

Hosting, technische und physische Infrastruktur

Schutz der Server und der Infrastruktur

- Minimale Nutzung öffentlicher IP-Adressen. Nur Front-End-Server haben öffentliche IP-Adressen.
- Firewalls sind vorhanden. Die Implementierung ist durch eine Richtlinie geregelt.
- Die Infrastruktur von Google Cloud Platform und Amazon Web Services mildert und absorbiert alle (D)DOS-Angriffe auf Layer 4 und darunter.
- Es gibt automatisierte und manuelle Prozesse zum Scannen und Erkennen von Schwachstellen in Server-Softwarepaketen und zur regelmäßigen Aktualisierung dieser Pakete.

Mandantenfähigkeit

- Das SaaS-Angebot von Tellent wird in einer mandantenfähigen, logisch getrennten Umgebung bereitgestellt. Dies bietet Skaleneffekte und bedeutet, dass Tellent viel in Maßnahmen investieren kann, um Ihr Konto vor Spitzenbelastungen zu schützen.
- Die logische Trennung wird durch das Qualitätssicherungsteam von Tellent und im Rahmen von Penetrationstests durch Dritte überprüft.
- Tellent bietet derzeit keine Single-Tenant-Lösungen an.

tellent

Protokollierung und Überwachung

- Viele Endnutzeraktivitäten können im Produkt verfolgt werden.
- Jeder API-Aufruf wird protokolliert. Die Tellent-Anwendungen basieren vollständig auf Interaktionen mit der/den API(s).
    - Tellent-Anwendungen bieten eine Audit-Protokollfunktion, die es Administratoren ermöglicht, Protokolle für eine Vielzahl von Ereignissen in der Anwendung einzusehen.
    - Für Recruitee SaaS:
        - Eine Liste der protokollierten Ereignisse finden Sie auf der folgenden Seite:
            - https://docs.recruitee.com/docs/audit-logs.
        - Weitere allgemeine Informationen über die Audit-Protokollfunktion finden Sie hier:
            - https://support.recruitee.com/en/articles/5661032-audit-logs.
    - Für KiwiHR SaaS:
        - Eine Anleitung zum Anzeigen eines Protokolls der Dateneingabe-Änderungen im Mitarbeiterprofil finden Sie hier:
            - https://support.kiwihr.com/en/articles/9345331-kiwihr-plus-features#h_624211bc16
    - Für Javelo SaaS:
        - Es ist möglich, den Fortschritt einer Kampagne zu verfolgen. Eine Anleitung, wie Sie die Berichte einsehen können, finden Sie hier:
            - https://support.javelo.com/en/articles/9345449-how-to-access-the-detailed-page-of-a-campaign
            - https://support.javelo.com/en/articles/9345600-how-does-the-my-team-tab-work
    - Bitte beachten Sie, dass nicht alle Protokolle über die Audit-Protokollfunktion verfügbar sind. Detaillierte Protokolle sind auf Anfrage erhältlich.
- Der Zugriff von Tellent-Mitarbeitern auf Kundenkonten wird protokolliert. Mitarbeiter können nur mit Erlaubnis des Endnutzers auf Konten zugreifen.
- Tellent-Anwendungen werden automatisch überwacht und Fehler werden rund um die Uhr von Tellent-Technikern untersucht.
    - Der Status der Tellent-Anwendungen kann unter https://status.tellent.com überwacht werden.
- Das Qualitätssicherungsteam richtet automatische Tests ein, um automatisch zu überprüfen, ob die Anwendung wie erwartet funktioniert.
- Der Zugriff auf Server, die von Tellent verwaltet oder kontrolliert werden, wird protokolliert.
- Intrusion-Detection-Systeme sind vorhanden.

Notfallwiederherstellung, Backup und Redundanz

- Tellent verfügt über eine Backup- und Wiederherstellungsstrategie.
- Die Webserver sind redundant und automatisch skalierbar.

- Das File-Hosting ist mit Amazon S3 hoch skalierbar.
- Verschlüsselte Backups aller Kundendaten werden mindestens täglich erstellt und gelöscht, wenn sie nicht mehr benötigt werden.
- Die Backups werden in mehreren Rechenzentren gespeichert.
- Alle Tellent-Rechenzentren verfügen über einen Notfallwiederherstellungsplan.

Hosting-Anbieter und Rechenzentren

- Tellent nutzt Google Cloud Platform und Amazon Web Services für das Hosting von Tellent-Anwendungen.
- Die von Google Cloud Platform und Amazon Web Services für Tellent bereitgestellten Dienste sind nach ISO 27001 und CSA STAR zertifiziert und entsprechen SOC 2 (SSAE 16/ISAE 3402 Typ II).
- Andere Hosting Subunternehmer oder Lieferanten sind ebenfalls nach ISO 27001 und/oder SOC 2 (SSAE 16/ISAE 3402 Typ I) zertifiziert.
    - Weitere Details finden Sie in unserem DPA.
- Alle Rechenzentren unterliegen strengen physischen Kontrollen.
- Alle Daten in den Rechenzentren werden professionell gelöscht, wenn die Hardware außer Betrieb genommen wird.

Büros

- Die Büros sind durch eine Kombination aus Kameras, Alarmanlagen, Sicherheitspersonal und/oder Schlüsselkarten/Schlüsselanhängern gesichert.
- Alle Mitarbeiter-Laptops werden vom Unternehmen verwaltet (MDM) und sind vor unbefugtem Zugriff geschützt.

Organisation und Management, Sicherheitsrichtlinien und -verfahren

- Die Mitarbeiter von Tellent sind verpflichtet, ihre Computerbildschirme zu sperren, wenn sie nicht an ihnen arbeiten.
- Tellent strebt ein papierloses Büro an.
- Alle Mitarbeiter von Tellent müssen sich zur Geheimhaltung verpflichten (z. B. durch ein NDA).
- Tellent-Mitarbeiter sind verpflichtet, nur sichere Passwörter zu verwenden.
- Die Geräte der Tellent-Mitarbeiter sind mit Antiviren-Software und Verschlüsselung ausgestattet.
- Es gibt Zugangskontrollrichtlinien, die sicherstellen, dass der Zugang widerrufen wird, wenn Tellent-Mitarbeiter das Unternehmen verlassen. Das Prinzip der geringsten Rechte wird angewendet und aktiv überwacht.
- Das Sicherheitsbewusstsein wird bei Tellent durch regelmäßige Schulungen aktiv aufrechterhalten.

Vorfallreaktion

- Tellent verfügt über einen Reaktionsplan für Sicherheitsvorfälle (SIRP).
- Der SIRP enthält eine klare Benennung der Zuständigkeiten, die im Falle eines Vorfalls zu ergreifenden Maßnahmen und eine Liste der internen und externen Mitglieder des Reaktionsteams.
- Der SIRP deckt auch Reaktionen auf Datenschutzverletzungen ab, wie in der Datenschutz-Grundverordnung vorgeschrieben.
- Mit den betroffenen Akteuren werden regelmäßig Übungen für den Fall eines Vorfalls (am runden Tisch) durchgeführt.

Service-Level und Support

- Tellent strebt eine wartungsfreie Betriebszeit von 99,5 % an. Die Erfolgsbilanz von Tellent finden Sie hier: https://status.tellent.com
- Das Support-Team von Tellent ist zwischen 9:00 und 18:00 Uhr CET und EST per E-Mail und Live-Chat erreichbar.
- Unsere Helpdesk-Artikel auf https://support.tellent.com bieten Anleitungen zu jedem Update.
- Größere Produktänderungen werden von unserem Support-Team per E-Mail und/oder In-App-Chat angekündigt.
- Produkt-Roadmaps finden Sie unter: https://support.tellent.com/en/articles/9805760-tellent-hr-platform-roadmap-2024

Definitionen

- Endnutzer: Alle Benutzer mit Ausnahme von Besuchern der Karriereseite, Bewerbern und Empfehlern.

Haftungsausschluss: Dieses Dokument soll dem Leser einen allgemeinen Überblick über die Sicherheits-, Compliance- und Betriebsmaßnahmen geben, die von Tellent in Bezug auf den/die Service(s) zum Zeitpunkt der letzten Aktualisierung getroffen wurden. Einige Unterschiede oder Nuancen können übersehen werden. Bitte kontaktieren Sie Tellent für spezifischere und/oder aktualisierte Informationen.