WhistleB

WHISTLEBLOWING CENTRE

Mai 2021

WhistleB: Kurzbericht zur Informationssicherheit

Qualitätskontrolle, Zertifikate und Bewertungen

WhistleB hat den Datenschutz zu unserer obersten Priorität gemacht. Der WhistleB-Dienst wird kontinuierlich überwacht und regelmäßig getestet, einschließlich Penetrationstests durch externe IT-Sicherheitsexperten. Besuchen Sie das WhistleB Trust Centre »um mehr über Hinweisgebersysteme und Datenschutz zu erfahren.

Assessments and Certifications

- ✓ Bewertungen und Zertifizierungen
- ✓ Einhaltung der EU-DSGVO. Externe Bewertung ISO 27001
- ✓ Konformität des ISMS nach ISO 27001. Externe Bewertung
- ✓ Schwachstellen- und Penetrationstests. Externe Zertifizierung
- ✓ Datenspeicherung und -entwicklung (Microsoft Azure): Azure verfügt über zahlreiche Zertifizierungen, darunter ISO 27001 und ISO 27018.

Externe Bewertungen

EU-Datenschutz-Grundverordnung (DSGVO) und ISMS (ISO 27001), externe Bewertungen:

„Insgesamt ist der WhistleB-Dienst des Unternehmens aus DSGVO-Sicht gut konstruiert. Zusätzlich zu seinem grundlegenden Design, das den strengsten Anforderungen entspricht, bietet der Dienst zahlreiche DSGVO-konforme Funktionen, wie z. B. die Möglichkeit selektiver Löschungen. Diese gelten als sehr fortschrittliche Funktionen und sind äußerst gut an die DSGVO-Anforderungen angepasst.“

„Das Sicherheitsniveau zum Schutz personenbezogener Daten (PII) entspricht den Branchenstandards sowie den Erwartungen und Anforderungen der Stakeholder.“ Die Konzepte „Privacy by Design“ und „Privacy by Default“ werden von der Richtlinienebene bis hin zu Entwicklung, Implementierung, Betrieb und Compliance-Aktivitäten angewendet. Technische Lösungen, einschließlich der WhistleB-Anwendung, werden nach Branchen- und IT-Sicherheitsstandards entwickelt und gepflegt. Erweiterte IT-Sicherheitskompetenzen für das Anwendungsmanagement werden beschafft und aufrechterhalten.

Jurgen von Rosen, Senior Data Protection Consultant, April 2021. Zertifiziert CIPP/E und CIPM (IAPP).

Schwachstellen- und Penetrationstests, externe Zertifizierung:

„Zum Zeitpunkt der Bewertung blieb die Privatsphäre der Hinweisgeber gewahrt. Outpost24 griff die Anwendung aus dem Internet an und konnte keine sensiblen Daten abrufen."
Datensicherheitsexperte Outpost24, Schwachstellen- und Penetrationstest, April 2021.

Geschäftsethik von WhistleB in Kürze

WhistleB verfügt über langjährige Erfahrung in Unternehmensethik und Nachhaltigkeit. WhistleB bietet Dienstleistungen im Zusammenhang mit der Einführung und Verankerung von Verhaltenskodizes, ethischen Richtlinien und Nachhaltigkeitsberichterstattung.

- ✓ WhistleB berichtet über seine Nachhaltigkeitsarbeit gemäß der Global Reporting Initiative (GRI).
- ✓ Alle Mitarbeitenden und Subunternehmer unterzeichnen den WhistleB-Verhaltenskodex/Lieferantenkodex.
- ✓ WhistleB kompensiert die durch das Unternehmen verursachten CO_2-Emissionen, deren Hauptquelle Geschäftsreisen sind.
- ✓ WhistleB ist Unterzeichner des UN Global Compact https://www.unglobalcompact.org/what-is-gc/participants/134882-WhistleB-Whistleblowing-Centre

Technische Informationen, Beispiele zentraler Lösungen

Der Hinweisgeberservice ermöglicht es Mitarbeitenden und anderen Stakeholdern, anonym oder offen eine Meldung über ein Anliegen einzureichen. Benannte Personen erhalten eine Benachrichtigung und melden sich im Fallmanagement-Tool an, um die Meldung zu lesen und Maßnahmen zu ergreifen.

Verschlüsselung

Daten sind nur über das Fallmanagement-Tool zugänglich, wobei der Zugriff nur autorisierten Nutzern gewährt wird. Das WhistleB-System verwendet eine Kombination aus symmetrischer und asymmetrischer Kryptografie, um alle Meldungen, Rückfragen und Übersetzungen zu verschlüsseln. Diese Methode ist sicher und stellt sicher, dass nur der vorgesehene Empfänger auf die Daten zugreifen kann.

WhistleB verarbeitet ausschließlich verschlüsselte Daten und kann Meldungen von oder an Hinweisgeber nicht entschlüsseln. Der Kunde kontrolliert den Verschlüsselungsschlüssel und ist die einzige Partei, die Daten entschlüsseln und darauf zugreifen kann. Auf mobilen Geräten werden keinerlei Daten gespeichert. Zusätzlich werden Kundendaten auf Dateiebene mit Transparent Data Encryption (TDE) verschlüsselt.

Zugriff

Die Anwendung unterstützt eine integrierte starke Authentifizierung basierend auf dem .NET-Authentifizierungsschema.

- WhistleB-Administratoren: Zugriff mit E-Mail-Adresse und persönlichem Passwort (vom Nutzer definiert) sowie Zwei-Faktor-Authentifizierung.
- Kundenzugriff: Zugang mit E-Mail-Adresse und persönlichem Passwort (vom Nutzer definiert). Zwei-Faktor-Authentifizierung kann optional aktiviert und erzwungen werden. Ein „sekundäres Passwort“ wird zum Entschlüsseln und Öffnen von Fällen verwendet.
- Das WhistleB-System erzwingt starke Passwörter.

Protokollierung (Logging)

- Kommunikationskanal (Hinweisgeber): Daten zu Hinweisgebern werden nicht nachverfolgt, um Anonymität sicherzustellen.
- Fallmanagement-Tool: Der Kunde kann die Fallbearbeitung über das interne Fallprotokoll nachverfolgen, d. h. Aktionen des Fall- oder Sicherheitsmanagers.
- WhistleB-Administratoren: Alle Logins werden protokolliert. Administratoren haben keinen Zugriff auf Kundendaten.

Sicheres Hosting

Die von WhistleB verwendeten Azure-Dienste werden in Rechenzentren betrieben, die für einen 24/7/365-Betrieb ausgelegt sind und Maßnahmen zum Schutz vor Stromausfällen, physischem Eindringen und Netzwerkausfällen einsetzen. Kundendaten werden durch verschlüsselte Kommunikation sowie durch Bedrohungsmanagement und -minderung, einschließlich regelmäßiger Penetrationstests, geschützt.

Daten werden innerhalb der EU/EWR gespeichert: primärer Standort in Irland, sekundärer Standort (Failover) in den Niederlanden.

Microsoft Azure verfügt über jährliche Zertifizierungen nach ISO/IEC 27001 (Informationssicherheitsmanagement) und ISO/IEC 27018 (Schutz personenbezogener Daten in der Cloud). Sicherheits- und Compliance-Erklärungen sind im Microsoft Trust Center verfügbar.