SpeakUp®

→ buyers guide

So finden sie das beste Whistleblowing-System für Ihre Organisation Ein Käuferleitfaden

Mit kostenlosen Vorbereitungsfragen und einer Software-Checkliste

Inhalt

SpeakUp®

Vorwort

Die Botschaft ist klar: Organisationen müssen die Verantwortung für ihren sozialen und ökologischen Fußabdruck übernehmen. Es ist erfrischend zu sehen, dass eine Kultur der Offenheit in so vielen Ländern der Welt zur neuen gesellschaftlichen Norm werden könnte.

Die EU scheint besonders entschlossen zu sein, die Bedingungen innerhalb wie außerhalb ihrer Grenzen zu verbessern. Die bekannte Richtlinie zum Schutz von Hinweisgebern und die geplante Richtlinie über die Sorgfaltspflicht von Unternehmen im Bereich der Nachhaltigkeit beweisen: Unternehmen tun gut daran, von sich aus soziale und ökologische Verantwortung zu zeigen.

Suchen Sie einer umsetzbaren Lösung für die Meldung von Missständen in Ihrer Organisation? Das ist gutes Timing! Der weltweite Markt für Whistleblowing-Software ist in voller Blüte. Er wächst enorm und wird bis 2028 voraussichtlich ein Volumen von mehr 170 Mrd. US-Dollar übersteigen.

Angesichts der vielen Alternativen müsste es relativ einfach sein, geeignete Mechanismen für Ihre Organisation zu finden. Doch der Hype um das Thema ist genau der Grund, dass es immer schwieriger wird, die richtige Lösung zu finden.

Wegen des starken Wachstums der Branche kommen ständig neue, noch nicht erprobte Lösungen auf den Markt. Diese verschleiern den eigentlichen Kern des Whistleblowings – nämlich dass es zur Selbstverständlichkeit werden sollte, Fehlverhalten in der Organisation durch Hinweise aufzudecken und zu verhindern.

Dieser Käuferleitfaden erklärt, was ein gutes Whistleblowing-Tool ausmacht. Er hilft Ihnen, in drei einfachen Schritten Ihr passendes Tool zu finden:

1. Verstehen Sie Ihre Organisation
2. Treffen Sie eine Vorauswahl
3. Vergleichen Sie Ihre Optionen

SpeakUp®

Worum geht es bei einem Whistleblowing-System wirklich?

Whistleblowing und Hinweise geben sind nicht immer dasselbe

Die EU-Kommission definiert Whistleblower als „Personen, die „Personen, die Informationen über Fehlverhalten, die sie in einem Arbeitskontext erhalten haben, innerhalb der betroffenen Organisation oder einer externen Behörde melden oder gegenüber der Öffentlichkeit offenlegen“ und so „zur Vermeidung von Schäden und zur Aufdeckung von Bedrohungen oder Schäden des öffentlichen Interesses“ beitragen, „die andernfalls unentdeckt blieben“.

Daher ist eine Meldung nur möglich, wenn bereits ein unangemessenes Verhalten festgestellt oder beobachtet wurde. Whistleblowing setzt ein Fehlverhalten voraus. Wie wäre es jedoch, wenn Sie nicht wartete, bis ein Fehlverhalten auftritt? Wenn Sie, statt Korrekturmaßnahmen zu ergreifen, proaktiv anfingen, eine Kultur der Offenheit zu schaffen?

Gute Regelungen und wirksame Mechanismen können Organisationen helfen, das Melden von Missständen zur Normalität zu machen. Hier kommt Ihre Whistleblowing-Lösung ins Spiel: Die Mitarbeitenden müssen wissen, wie sie ihre Bedenken äußern können und sich im Fall des Falles auch trauen. Dann wird Fehlverhalten auch verhindert und nicht nur korrigiert.

> Wenn alle sich trauen zu sprechen, muss niemand mehr laut werden.

→

SpeakUp®

Es geht also darum, die richtige Whistleblowing-Lösung zu finden:

Kultur

Es sollte ein grundlegendes Element der Organisationskultur sein, Missstände zu melden. Keine Whistleblowing-Lösung der Welt kann Sie vor Skandalen oder Rufschädigung bewahren, wenn sich niemand traut, sie zu nutzen und wenn einem Hinweis keine Maßnahmen folgen. Eine gesunde, offene und transparente Kultur ist daher eine Hauptvoraussetzung dafür, das beste Instrument zur Meldung von Missständen zu finden.

Offenheit

Wer die Wahrheit sagen will, muss zunächst das Whistleblower-Dilemma überwinden: die Abwägung zwischen Loyalität und Fairness. Genau deshalb sind einfache, unkomplizierte Mechanismen zur Meldung von Missständen am wirkungsvollsten. Es muss ganz einfach sein, den Dialog zu initiierren, damit es nicht als eine schwere, unangenehme Aufgabe empfunden wird, einen Hinweis zu geben. Daher sollte Ihr Whistleblowing-Tool Mitarbeitenden die Möglichkeit geben, sich in ihrer Muttersprache zu melden. Das wirksamste Instrument ist eines, auf das alle überall zugreifen können.

Anonymität

Oscar Wilde sagt: „Gib einem Mann eine Maske, und er wird dir die Wahrheit sagen“ Anonymität ist umstritten, aber für eine wirksame Meldung von Missständen zwingend erforderlich. Oft besteht die Befürchtung, dass Menschen die Anonymität als Maske benutzen, hinter der sie ungestraft falsche Anschuldigungen erheben können. Dennoch ist die Anonymität das beste Mittel, um ein Gefühl der Sicherheit zu schaffen. Das wirksamste Whistleblowing-Instrument verspricht nicht nur den Hinweisgeber-Schutz, es garantiert ihn auch.

SpeakUp®

Wie Sie ein passendes System finden

Da dieses Thema inzwischen zum Trend geworden ist, tauchen jeden Tag neue, unerfahrene Anbieter auf. Das überfordert viele Compliance-Teams, die das richtigen System zur Meldung von Missständen suchen.

Dabei ist es wichtig, dass ein einmal etablierter Whistleblowing-Mechanismus nicht ständig wieder geändert werden sollte. Allein die Beschaffung kann Monate dauern, und dabei sind Implementierung, Kommunikationskampagnen und Einführung noch nicht berücksichtigt. Noch wichtiger ist, dass Sie sich darüber im Klaren sind, dass die Wirksamkeit des Mechanismus vollständig von seiner erfolgreichen Einführung abhängt. Diese ist zeitaufwändig und der Erfolg ist nicht garantiert.

Die beste Lösung für Ihr Unternehmen finden Sie nur, wenn Sie sich Zeit nehmen, um Ihre Unternehmenskultur und Ihre Bedürfnisse zu verstehen. Bei diesem Projekt geht es nicht darum, welches Tool die meisten Punkte, am wenigsten Mühe macht oder am wenigsten kostet.

Ein Whistleblowing-System ist keine schnelle Lösung für die Einhaltung der Vorschriften. Vielmehr ähnelt sie einem vertrauenswürdigen und zuverlässigen Ethikberater: Sie hostet Ihre sensiblen Daten sicher; sie hilft Ihnen, die Unternehmenskultur zu stärken und Fehlverhalten zu bekämpfen.

Bevor Sie also mit der Vorauswahl beginnen, sollten Sie den Blick nach innen richten. Machen Sie sich ein Bild von der aktuellen Lage in Ihrer Organisation und denken Sie langfristig.

Diese drei Schritte helfen, Ihr Projekt zum Erfolg zu führen:

1. Verstehen
2. Qualifizieren
3. Vergleichen

Schritt 1:
Verstehen

Zunächst müssen Sie Ihr Unternehmen im Hinblick auf Kultur, Mitarbeitende und Projektanforderungen untersuchen. Dies mag nach übertriebenem Aufwand klingen, doch ein gutes Verständnis der Verhältnisse in der Organisation wird Ihren Aufwand bei der Beschaffung stark reduzieren und alle darauffolgenden Schritte beschleunigen.

Organisationskultur

Unter Organisationskultur verstehen wir alles, was Whistleblowing in Ihrer Organisation positiv oder negativ beeinflussen kann. Dazu gehören Ihr aktueller Verhaltenskodex und andere Richtlinien.

Denken Sie über den aktuellen Ansatz bei der Meldung von Missständen nach. Was steht in Ihrem Verhaltenskodex zu diesem Thema? Grundlage einer erfolgreiche Einführung Ihres Tools ist eine Kultur der Offenheit. Wenn Sie also noch keine Richtlinien zum Thema haben, sollten Sie diese erstellen. Außerdem sollten Sie sich mit möglichen Risiken befassen und herausfinden, welche anderen Bereiche Ihrer Organisationskultur verbessert werden können.

Wer sind die Hinweisgebenden? Ein umfassender Ansatz

Zweitens sollten Sie ein klares Bild von der Zielgruppe Ihres Whistleblowing-Tools haben. Die erste und wichtigste Gruppe sind die eigenen Mitarbeitenden. Damit meinen wir die gesamte Belegschaft: Vollzeit- und Teilzeitbeschäftigte, Freiberufler, Praktikanten und Ehemalige.

Darüber hinaus müssen Sie auch alle weiteren Personen berücksichtigen, die von Ihren Tätigkeiten betroffen sein könnten. Die geplante EU-Richtlinie über die Sorgfaltspflicht von Unternehmen (EU-Lieferkettenrichtlinie) wird Organisationen bald verpflichten, Risiken in ihrer gesamten Lieferkette zu identifizieren und zu mindern.

Sie sollten auch überlegen, ob Sie für Partner und Kunden eigene Kanäle einrichten. Auch wenn die Beziehungen weniger eng sind, können diese Gruppen dennoch von Ihren Aktivitäten betroffen sein und Ihrem Ruf schaden. Vor allem in großen multinationalen Unternehmen scheinen sich eigene Kommunikationskanäle für Kunden derzeit zu einer Best Practice zu entwickeln.

Wenn Sie anerkennen, dass Hinweise bei weitem nicht nur aus der eigenen Belegschaft kommen können, wird auch klar: Es ist von größter Bedeutung, einen unkomplizierten Mechanismus zur Meldung von Missständen zu finden. Wenn Sie sich ansehen, woher Hinweise tatsächlich kommen können, verstehen Sie auch die sprachlichen Anforderungen, denen Ihr Whistleblowing-System genügen muss. Welche Tools erleichtern die Kommunikation in allen relevanten Sprachen und können eine hochwertige, GDPR-konforme Darstellung für Ihre Sachbearbeitenden gewährleisten?

Neben der Sprache sollten Sie berücksichtigen, ob die Menschen mit der Technologie vertraut sind – dies ist ein direkter Indikator für Kommunikationspräferenzen. Wenn Hinweise z. B. hauptsächlich von Büroangestellten kommen, genügt wohl eine mobile Anwendung oder ein Onlineformular. Sind jedoch auch Menschen mit manuellen Tätigkeiten in der Gruppe, könnte ein Offline-Meldekanal erforderlich sein. →

Organisatorische Kapazitäten und Projektanforderungen

Das dritte wichtige Thema sind Ihre derzeitigen Kapazitäten und Projektanforderungen. Es könnte sein, dass Sie bereits ein System haben, das allerdings nicht besonders gut funktioniert. Warum ist deise Überlegung wichtig? Wenn Sie die aktuellen Probleme erkennen, werden Sie nicht zu einer anderen Lösung mit ähnlichen Einschränkungen wechseln.

Vielleicht haben Sie auch noch keine Erfahrung mit Whistleblowing-Systemen. Manchmal ist es besser, ganz von vorne anzufangen: So habe Sie ein gewisses Maß an Freiheit und Flexibilität. Fragen Sie sich, was Sie benötigen, um ein funktionierendes System aufzubauen. Überlegen Sie, wessen Unterstützung Sie brauchen könnten und holen Sie diese Personen ins Boot. Sie sollten auch überlegen, wie Sie am besten mit dem Tool und eingehenden Hinweisen umgeht. Wer wird wofür verantwortlich sein?

Denken Sie auch an alle Beteiligten, von denen Sie möglicherweise eine Genehmigung benötigen. In den meisten Unternehmen sind Compliance und Personalabteilung involviert. In einigen ist auch die Genehmigung der IT oder Beschaffung vorgeschrieben. In einigen Ländern gibt es auch andere lokale Verfahren und Anforderungen (z. B. Betriebsrat in Deutschland).

Nicht zuletzt sollten Sie den Zeitplan berücksichtigen. Wie lange dauert es, bis das Whistleblowing-System aktiv ist? Verkaufszyklus und Implementierungsverfahren können insgesamt 1-6 Monate dauern (je nach Größe des Unternehmens auch bis zu 1 Jahr). Mit einer guten Planung können Sie sich auf Unwägbarkeiten und plötzliche Verzögerungen vorbereiten und Fristen eher einhalten.

Schritt 2:
Qualifizieren

Wenn Sie die oben genannten Punkte geklärt haben, wird es viel einfacher sein, eine Vorauswahl zu treffen. Erkennen Sie z. B. in Schritt 1, dass ein Callcenter nicht zu Ihrer Kultur passt, können Sie in Schritt 2 einfach alle hotlinebasierten Systeme ausschließen.

Natürlich sollte Ihr System nicht nur kulturell und budgetär passen. Es muss auch einige nicht verhandelbare Anforderungen und Standards erfüllen. Deshalb ist es wichtig, bei der Vorauswahl stark auf Datenschutz, Sicherheit und Compliance zu achten.

Datenschutz

Datenschutz hat das Ziel, Daten vor unbefugtem Zugriff, Diebstahl oder Verlust zu schützen. Ihr Whistleblowing-System wird höchst sensible Daten speichern. Suchen Sie deshalb Anbieter mit einem angemessene Datenschutzprotokoll. Informieren Sie sich über die Anonymisierungs- und Verschlüsselungspraktiken der Anbieter. Bei cloudbasierten Lösungen stellt sich die Frage, wo die Server stehen. Wenn Sie die Informationen nicht online finden können, fragen Sie nach. Dies ist sehr wichtig für die Einhaltung der DSGVO, insbesondere, wenn ein Tool auch Übersetzungen ermöglicht.

Beim Datenschutz wäre es zum Beispiel eine sinnvolle Vorauswahl, wenn eine europäische Organisation US-Anbieter ausschließt. US-Gesetze (z. B. der Patriot Act) könnten nämlich Ihre sensiblen Daten in Gefahr bringen.

→

SpeakUp®

Sicherheit

Informationssicherheit bezieht sich auf die Methoden, Werkzeuge und Personal, die digitale Ressourcen eines Unternehmens schützen sollen. Versuchen Sie, Informationen über den Umgang des Anbieters mit Sicherheitsbedrohungen zu finden. Er sollte nachweisen können, dass strenge Sicherheitsprotokolle befolgt werden. Suchen Sie Anbieter, die folgende international anerkannte Standards für Informationssicherheit und Datenschutz kennen und nachweislich einhalten:

ISO27001:

Norm für Managementsysteme für Informationssicherheit (ISMS)

ISO27002:

Standard für ISMS, Cybersicherheit und Datenschutz - Informations Sicherheitskontrollen

ISO37002:

Whistleblowing-Management-Systeme - Leitlinien

Beachten Sie, dass diese Zertifizierungen meist 2-3 Jahre gelten. Sind sie also einmal erreicht, spielen sie für das Tagesgeschäft des Anbieters keine große Rolle mehr. Deshalb ist es wichtig, nur Anbieter zu berücksichtigen, die regelmäßige Audits durchführen und die Einhaltung der Standards lückenlos nachweisen. Der aktuell höchste internationale Prüfstandard für Whistleblowing-Anbieter ist der ISAE3000 Typ II. Er ist vergleichbar mit dem US-Standard SOC2. Er gewährleistet Datenschutz und Sicherheit auf hohem Niveau in allen Arbeitsbereichen.

Compliance

Auch wenn die Einhaltung der Vorschriften im Rahmen einer Kultur der Offenheit nur ein Hygienefaktor sein sollte, ist sie selbstverständlich notwendig. Welche Vorteile hätte die Einführung eines Mechanismus zur Meldung von Verstößen gegen die Vorschriften? Suchen Sie Lösungen, die Ihnen helfen, folgende EU-Vorschriften einzuhalten:

- DSGVO
- EU-Richtlinie zum Schutz von Hinweisgebern (Hinweisgeberrichtlinie)
- EU-Richtlinie zur Sorgfaltspflicht von Unternehmen im Bereich der Nachhaltigkeit (Lieferkettenrichtlinie)

Je nachdem, in welchen Ländern Sie tätig sind, müssen Sie auch lokale Rechtsvorschriften beachten, wie z. B.: Sapin II (FR), Lieferkettengesetz (DE) oder Public Interest Disclosure Act (UK).

Bei der Vorauswahl schließen Sie also unzureichende und riskante Lösungen aus. Die hier genannten Ratschläge sollen Ihnen diese Vorauswahl erleichtern - allerdings sollten Sie nicht nur noch auf diese Themen achten. Die Einhaltung der Vorschriften ist nicht gleichbedeutend mit einer wirksamen Implementierung. →

Schritt 3:
Vergleichen

Sobald Sie wissen, welche Whistleblowing-Tools überhaupt infrage kommen, können Sie mit dem Vergleich beginnen. Wählen Sie nun in Schritt 3 einige wenige Anbieter, deren System Sie im Rahmen einer Demo kennenlernen möchten.

Bedenken Sie: Compliance ist wichtig, aber sie garantiert keine effektive Implementierung. In der Vergleichsphase können Sie sich etwas intensiver mit Hintergrund und Ansatz des Anbieters befassen. Whistleblowing ist ein heikles Thema. Anbieter mit einer nachgewiesenen Erfolgsbilanz sind daher eher in der Lage, Ihre besonderen Anforderungen zu verstehen und zu berücksichtigen. Langjährige Erfahrung, die Vielfalt der Kunden und der allgemeine Ansatz biem Thema Whistleblowing sind gute Indikatoren für das Dienstleistungsniveau des Anbieters.

Die Schritte 1 und 2 des Käuferleitfadens bereiten Sie auf einen gründlichen Vergleich der gewählten Anbieter vor. In diesem Stadium haben Sie schon ein klares Verständnis für Ihre organisatorischen und projektbezogenen Bedürfnisse. Sie haben jene Lösungen identifiziert, die Ihnen helfen könnten, die Anforderungen zu erfüllen. Nun sind zwei oder drei Systeme in der engeren Wahl, die gut zu passen scheinen. Nun gilt es, Gespräche zu führen und sich von den Anbietern die Systeme zeigen zu lassen.

Wie Sie eine Produkt-Demo optimal nutzen

1. Bereiten Sie sich vor.

Demos können zeitaufwändig sein. Denken Sie daher vor dem Gespräch noch einmal über Ihren Whistleblowing-Prozess nach. Bereiten Sie Fragen vor, die auf die Bedürfnisse Ihres Fallbearbeitungsteams zugeschnitten sind. So können Sie die richtigen Fragen zu Zugriffsrechten und Arbeitsabläufen stellen. Es wird auch dem Anbieter auch helfen, die Möglichkeiten des Systems effektiv vorzuführen.

2. Beziehen Sie wichtige Interessengruppen ein.

Sie müssen diese Gespräche nicht allein führen. Alle, die überzeugt werden müssen, sollten in dem Gespräch vertreten sein. Dies können Personen aus dem Management, der IT oder der Beschaffung sein.

3. Sammeln Sie die richtigen Informationen.

Sammeln Sie in diesen Anrufen alles, was Sie für einen angemessenen Vergleich benötigen. Konzentrieren Sie sich auf diese 6 Kernbereiche: Kommunikation, Umgang mit Problemen, technische Anforderungen, Datenschutz und Sicherheit, Compliance und Support.

Fazit

SpeakUp unterstützt Organisationen seit 20 Jahren bei der Umsetzung von Whistleblowing-Prozessen. Wir wissen, wie eine Kultur der Offenheit entsteht – oder im Keim erstickt wird. Die Auswahl Ihres Whistleblowing-Tools ist keine leichte Aufgabe. Aber wenn Sie es richtig machen, müssen Sie es nur einmal tun. Die in diesem Leitfaden vorgeschlagenen Schritte helfen Ihnen, dieses Ziel zu erreichen.

Damit Sie schneller vorankommen, haben wir einen Vorbereitungsbogen für Schritt 1 sowie eine Software-Checkliste für die Schritte 2 und 3 zusammengestellt. Das klingt nach viel Arbeit? Stimmt. Aber es wird Ihnen später noch mehr Arbeit ersparen.

Wünschen Sie weitere Informationen, erreichen Sie uns unter +31 (0)20 471 2398.

SpeakUp®

Vorbereitungsbogen

Aus welchen Personenkreisen könnten Hinweisgeber kommen? (z. B. Mitarbeitende, Kunden, Partner, Lieferanten) Ihre Antwort

An wie vielen Standorten sind wir tätig und welche Sprachen benötigen wir? Ihre Antwort:

Wie viele Kanäle brauchen wir?

Welche Kanäle eignen sich am besten für die fraglichen Personenkreise (Telefon/App/Web)?

Welchen Ansatz verfolgen wir derzeit beim Thema Whistleblowing? Was können wir verbessern? Ihre Antwort

(falls zutreffend) Was sind die Schwächen unseres derzeitigen Systems und was sollte anders gemacht werden? Ihre Antwort

Wie werden wir eingehende Fälle bearbeiten?

Wessen Zustimmung benötige ich für die Auswahl eines Tools? (z. B. IT, Beschaffung, SEO, Betriebsrat)

Wer kann mir helfen, dieses Projekt zum Erfolg zu führen? Ihre Antwort

Wie lange dauert es, bis das Whistleblowing-System aktiv ist?

Whistleblowing-Software-Checkliste

1. Kommunikation

	SpeakUp®	Other
Weltweite Verfügbarkeit rund um die Uhr		
Sichere Kommunikation in beide Richtungen zwischen Hinweisgebenden und Organisation		
Anonymes automatisiertes telefonisches Einreichen von Hinweisen		
Anonymes Einreichen von Hinweisen online		
Anonymes Einreichen von Hinweisen über mobile Anwendungen		
Einreichen von Hinweisen via Callcenter (mit Personal)		
Optional: nicht-anonymes Einreichen von Hinweisen		
Benutzerfreundliche Oberfläche		
Berücksichtigt verschiedene Präferenzen beim Einreichen (z. B. Sprache oder Kommunikationskanal)		
Fördert den Dialog mit Freitext-Option		
Unterstützt Dateianhänge (z. B. Bilder, Videos, Dokumente)		
Integrierte Übersetzung und Transkription von Nachrichten		
Automatische maschinelle Übersetzung von Nachrichten		
Professionelle Übersetzung von Nachrichten (auf Nachfrage)		
Anzahl der angebotenen Sprachen		
Benachrichtigt Hinweisgebende über Änderungen des Berichts		
Benachrichtigt Sachbearbeitende über Änderungen des Berichts		
Sammelt Feedback über die Benutzererfahrung beim Einreichen von Hinweisen		
Individuell anpassbar an das Branding des Unternehmens		
Anpassbare Aufnahmeformulare		

SpeakUp®

2. Umgang mit „Issues“ (Hinweise)

	SpeakUp®	Other
Anpassbare Berichtskanäle je nach Art des im Hinweis genannten Problems		
Unterstützt Hinweise über Offline-Kanälen (z. B. E-Mail, Vorschlagsbox)		
Automatische Problem-Sortierung anhand vordefinierter Kriterien		
Berücksichtigung organisatorischer Hierarchien und Strukturen		
Anpassbare Benutzerrollen und Zugriffsberechtigungen		
Werkzeuge für die Zusammenarbeit (z. B. Kommentare, Aufgaben)		
Automatische Benachrichtigung bei Aufgabenaktualisierungen und Statusänderungen		
Sichere Speicherung von Dateianhängen, die als Beweismittel verwendet werden können		
Datenexport/-import in verschiedenen Formaten (z. B. CSV, JSON)		
Registriert alle Maßnahmen zur Problembehandlung		
Hilft bei der Dokumentation von Lösungen und dem Schließen von Fallakten		
Erleichtert Eskalation bei ungelösten Problemen		
Datenvisualisierung und Berichtsfunktionen		
Instrumente zur Fall- und Trendanalyse		
Verfolgung von Metriken und KPIs zur Wirksamkeit des Programms		
Vorgefertigte und anpassbare Berichtsvorlagen		
Unterstützung bei regelmäßigen Prüfungen von Programmen zur Problembehandlung		
Instrumente zur Risikobewertung und Planung von Maßnahmen zur Minimierung von Risiken		
Anpassbare Risikokategorien und Klassifizierungsschemata		
Alle Daten sind jederzeit für den Export verfügbar		

3. Technische Fragen

	SpeakUp®	Other
Kontinuierliche Systemaktualisierungen		
Kompatibilität mit mehreren Geräten (Desktop, Handy, Tablet)		
Integration mit bestehenden Unternehmensanwendungen		
Integration mit E-Mail-Systemen zur nahtlosen Weiterleitung von Berichten		
Integration mit bestehenden Sicherheits- und Zugangskontrollsystemen (SSO)		
Integration mit Präventionsinstrumenten und -diensten von Drittanbietern		
Integration mit Business Intelligence-Tools (z. B. Power BI, Tableau)		
Integration mit Projektmanagement-Tools (z. B. Trello, Asana)		
Geolokalisierung und Verfolgung von IP-Adressen (mit Zustimmung)		
Unterstützt Datenimporte aus anderen Tools		

4. Datenschutz & Sicherheit

	SpeakUp®	Other
Datenspeicherung in der EU		
Anpassbare Richtlinien zur Datenaufbewahrung und -archivierung		
Einhaltung von Datenschutzbestimmungen (z. B. DSGVO, CCPA)		
Praktiken zur Datenminimierung und Speicherbegrenzung		
Sichere Datenspeicherung, -übertragung und Verschlüsselungsprotokolle		
Techniken zur Anonymisierung und Pseudonymisierung von Daten		
System zur Erkennung von Datenschutzverletzungen sowie Benachrichtigung und entsprechenden Reaktion		
Verwaltung der Rechte von Betroffenen (z. B. Recht auf Auskunft, Löschung, Richtigstellung/Gegendarstellung)		
Sichere Verfahren zur Datensicherung und -wiederherstellung		
Datenschutzfreundliche Auditing- und Protokollierungsverfahren		
Multi-Faktor-Authentifizierung (MFA) für den Benutzerzugang		
Regelmäßige Sicherheitsaudits und Schwachstellenbewertungen		

SpeakUp®

5. Compliance

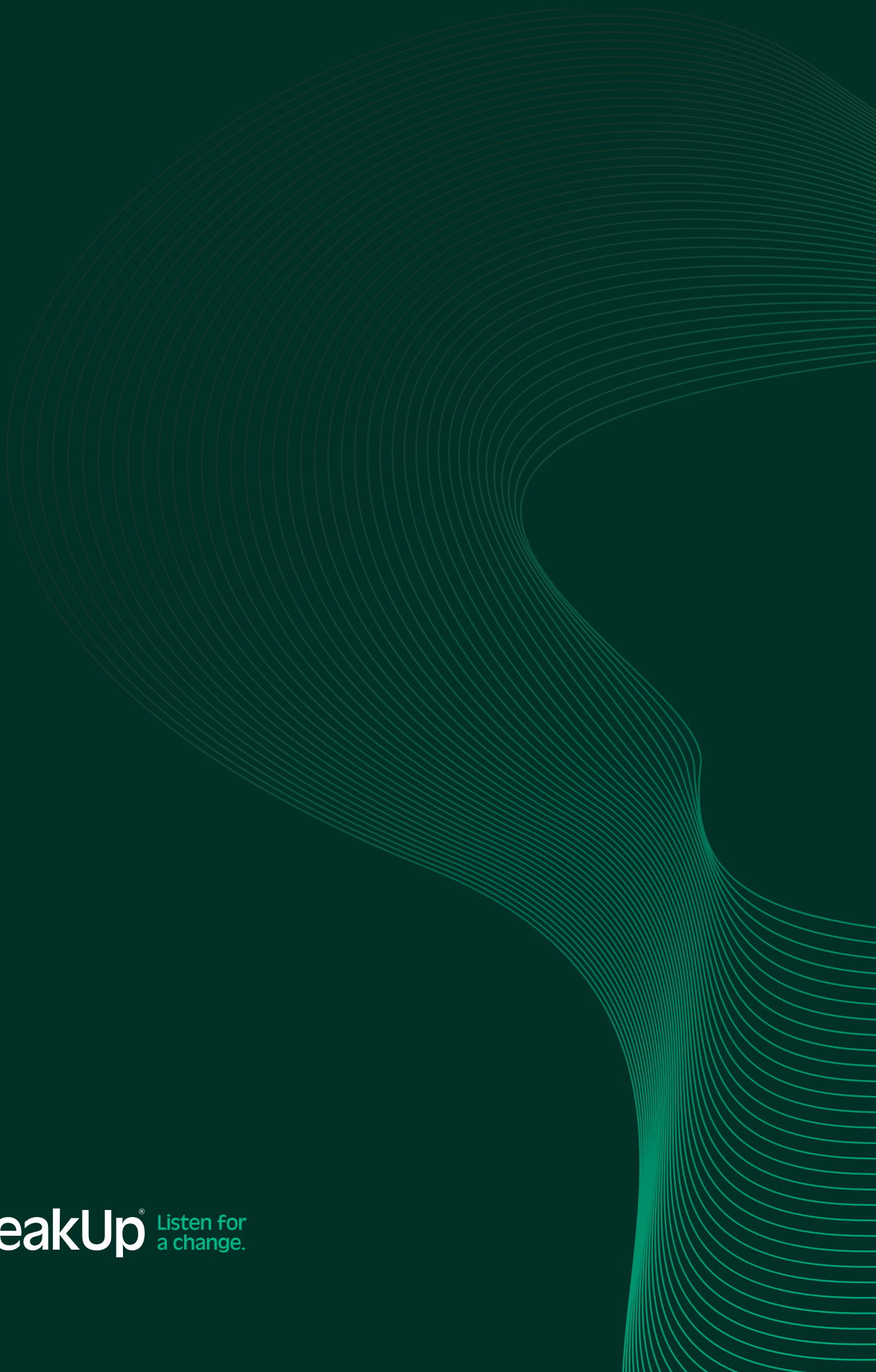
	SpeakUp®	Other
DSVGO		
Die EU-Hinweisgeberrichtlinie		
ISO27001		
ISO27002		
ISO27701		
ISAE3000 Type I		
ISAE3000 Type II (entspr. SOC2)		
Jährliche Pen-Tests		

6. Support

	SpeakUp®	Other
Zügige Systemeinführung		
Personalisiertes Onboarding		
Nachgewiesene Erfolgsbilanz und Erfolgsgeschichten von Kunden		
Bewährte Praktiken & Beispielmaterial		
Branchenspezifisches Knowhow und maßgeschneiderte Lösungen		

info@speakup.com
+31 (0)20 662 15 45

Olympisch Stadion 6, 1076 DE
https://speakup.com



SpeakUp® Listen for a change.