PRESSEMITTEILUNG

Whistleblowing-Plattform nutzen: Was Arbeitnehmer und Unternehmen beachten müssen

Berlin, 15. April 2021 – Zum Ende des Jahres 2021 wird das deutsche Gesetz zum Whistleblower-Schutz in Kraft treten: Unternehmen mit mehr als 50 Angestellten bzw. einem Jahresumsatz von 10 Mio. Euro müssen verpflichtend Hinweisgebersysteme einführen. Was Arbeitnehmer*innen sowie Unternehmen bei einer Whistleblowing-Plattform beachten sollten, weiß Whistleblowing-Experte Kai Leisering von Business Keeper (www.business-keeper.com), dem europäischen Marktführer für elektronische Hinweisgebersysteme.

Empfehlungen für Arbeitnehmer*innen

- **EU-Whistleblowing-Richtlinie:** Noch sind Whistleblower in Europa und Deutschland nicht ausreichend geschützt: Häufig haben sie für die Meldung eines Missstandes mitunter schwerwiegende Konsequenzen zu befürchten. Das Bundesjustizministerium hat deswegen bis Ende des Jahres Zeit, das deutsche Gesetz zum Whistleblower-Schutz umzusetzen. Die Richtlinie verpflichtet Unternehmen mit mehr als 250 Angestellten bzw. einem Jahresumsatz von 10 Millionen Euro, ab 2023 dann auch Unternehmen mit über 50 Angestellten, staatliche Institutionen und Gemeinden ab einer bestimmten Größe zur Einführung einer Whistleblowing-Plattform.

- **Hinweisgebersystem oder Öffentlichkeit?** Vorerst ist der Schutz von Hinweisgebenden im Falle der Veröffentlichung von Missständen nicht endgültig geregelt. Aus diesem Grund empfiehlt sich eine interne Meldeabgabe im Unternehmen, statt die Meldung an die Öffentlichkeit zu tragen.

- **Welche Missstände dürfen gemeldet werden?** Zu den am stärksten verbreiteten Missständen zählen unter anderem die Verletzung von internen Richtlinien und Regelungen (“Code of Conduct”), Verstöße gegen das allgemeine Gleichbehandlungsgesetz, Diskriminierung, Korruption, Diebstahl, Betrug und Wettbewerbsverstöße.

- **Sichere Hinweisabgabe**: Um die Anonymität zu wahren, sollten Meldende keine persönlichen Daten angeben, wie ihren Namen oder ihr Verhältnis zu den Täter*innen. Auch sollten keine sonstigen Inhalte in die Meldung einfließen, die Rückschlüsse auf die eigene Person zulassen könnten. Zudem sollte unbedingt auf eine sichere Internetverbindung geachtet werden: Diese ist am Schloss-Symbol in der Adresszeile des Browsers erkennbar. Hinweisgebende sollten nach Möglichkeit nicht die eigenen Arbeitsgeräte nutzen.

- **Beweislage prüfen**: Wenn Missstände gemeldet werden, empfiehlt es sich, Beweisstücke zur Hand zu haben. Bei der Ermittlung des Missstandes können diese eine essenzielle Rolle spielen und die Hinweisgebenden absichern.

Empfehlungen für Arbeitgeber und Unternehmen

- **Verzicht auf Cloud-Anbieter**: Bei der Wahl eines Anbieters von elektronischen Hinweisgebersystemen sollte darauf geachtet werden, dass dieser die Daten nicht in einer Cloud aufbewahrt. Eine Alternative dazu bieten zum Beispiel Hochsicherheitsrechenzentren, um ein Datenleck zu verhindern.

- **Anonymität**: Im Fokus einer Whistleblowing-Plattform sollte die Anonymität der meldenden Person stehen: Die Daten sollten ausschließlich für die Meldenden selbst sowie für die Fallbearbeiter*innen zugänglich sein. Einsicht in die Daten sollten weder Mitarbeitende der Polizei noch Staatsanwaltschaft erhalten, um die Identität der Hinweisgeber*innen zu schützen.

- **Missbrauch vs. Verantwortung:** Oftmals befürchten Arbeitgeber*innen einen Missbrauch der Plattform, zum Beispiel, um unliebsame Kolleg*innen zu denunzieren. Erfahrungsgemäß wird die Anonymität eines Hinweisgebersystems jedoch dafür genutzt, auf reale Missstände hinzuweisen und dient somit dem Wohl des Unternehmens. Unternehmen können in den Hinweisgebersystemen auch Hinweiskategorien als Unterstützung hinterlegen, um zu verhindern, dass jedes kleinste Vergehen gemeldet wird.

- **Transparenz und Vertrauen:** Zudem sorgt das Angebot eines Hinweisgebersystems bei Arbeitnehmer*innen für Vertrauen: Das Unternehmen kommuniziert, dass es um Transparenz bemüht ist und bezieht sämtliche Mitarbeitenden, Partner*innen und Kunden in den Prozess einer ethischen Unternehmensführung ein.

- **Interne Konfliktlösung**: Business Keeper empfiehlt, jegliche Missstände nach Möglichkeit intern zu lösen. Wird der Fall intern ernst genommen und bearbeitet, besteht für Hinweisgebende keine Notwendigkeit, sich an externe Parteien bzw. an die Öffentlichkeit zu wenden. Dringen einmal sensible Informationen nach außen, kann dies zu erheblichen Reputationsschäden führen und geht häufig mit großen finanziellen Einbußen einher.

ÜBER BUSINESS KEEPER

Die Business Keeper GmbH (www.business-keeper.com) ist der europäische Marktführer für elektronische Hinweisgebersysteme und Compliance-Software. Seit 2001 entwickelt das Berliner Unternehmen innovative Integritäts- und Compliance-Anwendungen gegen Wirtschaftskriminalität wie Korruption, Geldwäsche und andere gesellschaftliche Missstände. Das BKMS® (Business Keeper Monitoring System) Compliance System ist modular aufgebaut: Neben dem herkömmlichen Hinweisgebersystem kann die BKMS® Plattform Drittparteien überprüfen sowie helfen, weitere Genehmigungsprozesse einzuhalten. Speziell für KMUs wurde das Incident Reporting Essentials entwickelt: Dieses können Unternehmen und Organisationen in wenigen Minuten eigenständig konfigurieren.

Die doppelte Verschlüsselung der Meldedaten gewährleistet Hinweisgebenden höchste Sicherheit. Die Compliance-Plattform BKMS® Compliance System von Business Keeper ist EU-DSGVO-konform und die umfassendste und erste Compliance Lösung weltweit, die nach den strengen EuroPriSe-Kriterien zertifiziert ist. Zum Kundenstamm des Unternehmens zählen zahlreiche börsennotierte Konzerne aus Europa sowie Behörden, Kindeswohl-Einrichtungen und NGOs. Business Keeper beschäftigt 100 Mitarbeiter*innen in Berlin und verfügt über weitere Büros in Augsburg, Madrid und Paris.

Pressekontakt:
Luisa Lindenthal I luisa.lindenthal@tonka-pr.com I +49.30.403647.613
Miriam Goldman I miriam.goldman@tonka-pr.com I +49.30.403647.623