25. Februar 2023
von Mag. Sergej Jaklitsch, MBA

Das Hinweisgeberschutzgesetz ist am 25. Februar 2023 in Kraft getreten – wichtige Fragen für Unternehmen zusammengefasst

Das lang erwartete Hinweisgeberschutzgesetz (HSchG) ist am 01. Februar 2023 vom Nationalrat beschlossen worden. In der Bundesratssitzung am 16. Februar 2023 erteilte der Bundesrat seine Zustimmung zum neuen Gesetz. Im Anschluss wurde das Gesetz am 24. Februar 2023 im Bundesgesetzblatt BGBl. I Nr. 6/2023 kundgemacht und ist in Folge am 25. Februar 2023 in Kraft getreten.

Was bedeutet das Gesetz nun konkret für Ihr Unternehmen? Worauf muss geachtet werden? Die wichtigsten Fragen:

Wer ist betroffen und welche Übergangsfristen gibt es?

Generell sind durch das Gesetz alle Unternehmen **ab 50 Mitarbeitern** verpflichtet, Hinweisgebersysteme einzuführen. Für Unternehmen **ab 250 Mitarbeitern** gilt für die Implementierung eines internen Hinweisgebersystems eine **Übergangsfrist von sechs Monaten** ab dem Inkrafttreten dieses Gesetzes, das heißt **ab dem 25. Februar 2023.** Größere Unternehmen müssten daher bis 25. August 2023 handeln. Für Unternehmen mit **mindestens 50, aber weniger als 250 Mitarbeitern** gibt es eine Übergangsphase **bis zum 17. Dezember 2023.**

Kann für Töchterunternehmen das Hinweisgebersystem der Konzernmutter genutzt werden?

Die Arbeitnehmerschwelle gilt für jede Tochtergesellschaft separat und nicht konzernweit. Konzernunternehmen können aber die Meldestelle zentral bei der Konzernmutter ansiedeln. Allerdings verbleibt die Bearbeitung aller eingegangenen Meldungen bei dem jeweiligen Tochterunternehmen als Verantwortliche. Es besteht lediglich eine gemeinsame Verantwortlichkeit für den technischen Betrieb. Insbesondere für Konzerne und Unternehmensgruppen interessant und nützlich ist hierbei ein digitales Hinweisgebersystem mit Mandantenfähigkeit und einer Nutzerrechtevergabe. Somit können mehrere Tochtergesellschaften in einem System dargestellt werden, auch wenn das Hinweisgebersystem bei der Mutter-gesellschaft angesiedelt ist. Eingehende Fälle, die zugehörigen Akten und die Berechtigungen können den Tochtergesellschaften bzw. Organisationseinheiten zugeordnet werden. Zudem besteht die Möglichkeit, dass diese Gesellschaften mit einer eigenen Meldeplattform vertreten sind.

Welche Meldekanäle können genutzt werden?

Die Meldungserstattung des Hinweisgebers muss schriftlich (zum Beispiel Meldeplattform) oder mündlich und auf Wunsch auch persönlich möglich sein. In der Praxis geht die Tendenz schon allein wegen der Skalierbarkeit in Richtung technische Hinweisgeber-systeme, die rund um die Uhr verfügbar sind. Des Weiteren kann eine technische Lösung effektiver und kostengünstiger sein. Digitale Hinweisgebersysteme, die Anonymität sicherstellen, senken die Hemmschwelle für Hinweisgeber. Je niedriger die Hemmschwelle, desto wahrscheinlicher ist es, dass die Unternehmen von wertvollen

Hinweisen profitieren. Ein internes Hinweisgebersystem muss vor allem Vertrauen schaffen und einfach sein im Unternehmen. Ein weiterer Vorzug ist, dass digitale Hinweisgebersysteme schnell implementierbar sind und zu überschaubaren Kosten - monatliche SaaS-Gebühr - betrieben werden.

Können sich Hinweisgeber auch direkt an die zuständige externe Behörde wenden?

Zu beachten ist schließlich auch die Gleichwertigkeit der internen und externen Meldung: Das neue Gesetz sieht keine unternehmens-interne Meldeverpflichtung vor. Dem Hinweisgeber ist freigestellt, ob er sich zuerst an eine interne oder externe Meldestelle wendet. Eine interne Meldung liegt im Interesse des Unternehmens. Das Unternehmen behält dadurch die Kontrolle, kann prüfen, Maßnahmen ergreifen und Missstände beseitigen, bevor Behörden den Fall aufnehmen oder die Presse berichtet und somit Unternehmenserfolg und Reputation beschädigt werden. Die externe zentrale Meldestelle (sog. One-stop-shop) für den privaten und öffentlichen Sektor ist im vorliegenden Gesetz das Bundesamt zur Korruptionsprävention und -bekämpfung. Durch eine einheitliche Anlaufstelle sollen Hinweisgeber davon befreit werden, sich mit komplexen Zuständigkeitsfragen auseinandersetzen zu müssen.

Wer kann als Meldestelle fungieren?

Für die Wahrnehmung dieser Funktion kann jede unparteiische, weisungsfreie Person oder Abteilung im Unternehmen fungieren. Dafür eignen sich beispielsweise ein Datenschutzbeauftragter, Compliance Officer, die Compliance-, Rechtsabteilung, Interne Revision, ein Auditverantwortlicher, ein Vorstandsmitglied oder

Finanzvorstand, aber auch externe Berater. Eine Doppelfunktion ist zulässig. So kann beispielsweise ein Datenschutzbeauftragter diese Aufgabe übernehmen, solange die Unabhängigkeit gewahrt bleibt.

Muss die Meldestelle auch die Leitung eines Unternehmens informieren?

Nach dem Hinweisgeberschutzgesetz ist die interne Meldestelle berechtigt die Geschäftsführung bzw. den Vorstand von den Inhalten eines innerhalb des Unternehmens gegebenen Hinweises zu verständigen, wenn die Überprüfung des Hinweises den begründeten Verdacht einer Rechtsverletzung ergibt, die Verständigung geeignet erscheint, von vergleichbaren künftigen Rechtsverletzungen abzuhalten und mit einer Gefährdung der Folgemaßnahmen als Folge der Verständigung nicht zu rechnen ist. Die Identität des Hinweisgebers ist jedoch von der internen Stelle der Leitung des Unternehmens gegenüber jederzeit geheim zu halten.

Welche Fristen müssen hinsichtlich der Fallbearbeitung eingehalten werden?

Unternehmen müssen Fristen nach Empfang eines Hinweises sicherstellen. Innerhalb von 7 Tagen muss der Eingang des Hinweises bestätigt werden. Innerhalb von 3 Monaten nach Eingangsbestätigung oder 7-Tage-Frist muss eine qualifizierte Rückmeldung über geplante bzw. bereits ergriffene Folgemaßnahmen samt Begründung an den Hinweisgeber erfolgen. Darüber hinaus sind alle eingegangenen Meldungen umfassend zu dokumentieren.

Was ist der sachliche Anwendungsbereich des Hinweisgeberschutzgesetzes?

Zum sachlichen Anwendungsbereich zählen das Vergaberecht, Finanzdienstleistungen, Finanzprodukte, die Finanzmärkte, Verhinderung von Geldwäsche- und Terrorismusfinanzierung, das Verbraucher-, Datenschutzrecht, die Produkt- und Verkehrssicherheit, der Umweltschutz, die Strahlen- Lebensmittel- und Futtermittel-, Tiergesundheit sowie die Sicherheit von Netz- und Informations-systemen und die öffentliche Gesundheit. Ausgedehnt wurde der Anwendungsbereich auf die Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 des Strafgesetzbuches wie beispielsweise Missbrauch der Amtsgewalt, Geschenkannahme oder Bestechung.

Welche Personen werden geschützt?

Das Hinweisgeberschutzgesetz umfasst alle Personen, die im Rahmen ihrer beruflichen Tätigkeit von Missständen in einem Unternehmen Kenntnis erlangt haben. Geschützt sind neben den Arbeitnehmern auch ehemalige Arbeitnehmer, Stellenwerber, bezahlte und unbezahlte Praktikanten, Volontäre, Arbeitnehmer von Auftragnehmern und Lieferanten, Selbständige sowie Anteilseigner und Personen in Leitungs- oder Aufsichtsorganen.

Welche Bedingungen gelten für den Schutz von Hinweisgebern?

Der Hinweisgeber muss hinreichenden Grund zu der Annahme haben, dass die gemeldeten Informationen zum Zeitpunkt der Meldung der

Wahrheit entsprachen und in den Geltungsbereich dieses Gesetzes fallen.

Wer trägt die Beweislast bei einem Verstoß gegen das Repressalienverbot?

Mit dem neuen Gesetz genießen Hinweisgeber einen gesetzlichen Schutz und dürfen aufgrund der Hinweisabgabe keine Repressalien wie Kündigung, Versagung einer Beförderung, Minderung des Entgelts, Disziplinarmaßnahmen oder Mobbing erleiden. Landet ein Fall vor Gericht, gilt das Prinzip der Beweislastumkehr: Das von der Meldung betroffene Unternehmen muss nachweisen, dass es keine Vergeltungsmaßnahmen gegen den Hinweisgeber gesetzt hat. Unter anderem müssen Arbeitgeber somit beweisen, dass es sich bei der Kündigung eines Mitarbeiters um keine Vergeltungsmaßnahme handelt und kein Zusammenhang mit dem Hinweis besteht.

Welche Vertraulichkeitsanforderungen müssen Unternehmen erfüllen?

Unternehmen müssen Meldekanäle anbieten, die so sicher konzipiert sind, dass die Vertraulichkeit der Identität des Hinweisgebers gewahrt bleibt. Die vertrauliche Behandlung der Identität des Hinweisgebers ist somit oberstes Gebot. Die Identität des Hinweisgebers darf nur dem für die Meldung zuständigem Bearbeiter und den absolut erforderlichen hinzugezogenen Mitarbeitern oder Beratern bekannt sein, wie beispielsweise Personen aus der IT, Rechts- und Buchhaltungsabteilung. Nur in besonderen Fällen darf die Identität des Hinweisgebers oder der betroffenen Person einer Meldung offengelegt werden, zum Beispiel im Rahmen behördlicher Untersuchungen, eines verwaltungsbehördlichen oder gerichtlichen

Verfahrens. **Gehen Meldungen anonym ein, impliziert das, dass ein Verstoß gegen das Vertraulichkeitsgebot gar nicht erst möglich ist.** Eine Möglichkeit dazu ist der Betrieb eines Meldekanals, der anonyme Kommunikation ermöglicht.

Muss ein Hinweisgebersystem anonyme Meldungen ermöglichen?

Das Hinweisgeberschutzgesetz begründet eine Pflicht für Unternehmen, anonyme Meldungen entgegen zu nehmen und solche Meldungen zu bearbeiten. In der Praxis machen anonyme Meldungen einen erheblichen Teil der Meldungen aus. Zudem veranlasst ein leicht bedienbarer Meldekanal, der Anonymität sicherstellt, Hinweisgeber zur Preisgabe ihres Wissens.

Was muss aus datenschutzrechtlicher Sicht bei der Nutzung von Hinweisgebersystemen beachtet werden?

Nach dem Hinweisgeberschutzgesetz sind personenbezogene Daten ab ihrer letztmaligen Verarbeitung oder Übermittlung fünf Jahre und darüber hinaus solange aufzubewahren, als es zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der StPO erforderlich ist. Nach Entfall der Aufbewahrungspflicht sind personenbezogene Daten zu löschen. Protokolldaten sind ab ihrer letztmaligen Verarbeitung oder Übermittlung bis zu drei Jahren nach Entfall der Aufbewahrungspflicht aufzubewahren bzw. zu speichern. Ferner ist bei Datenverarbeitungen auf Grundlage des Hinweisgeberschutzgesetzes keine Datenschutz-Folgenabschätzung durchzuführen. Wird das Hinweisgebersystem von einem

Dienstleister (SaaS) zur Verfügung gestellt, ist noch eine Auftragsverarbeitervereinbarung mit diesem abzuschließen.

Ergänzend für Konzernunternehmen ist zu berücksichtigen: Jedes Unternehmen innerhalb eines Konzerns wird bei der Verarbeitung von personenbezogenen Daten als eigenständige Verantwortliche angesehen. Ist nun das Hinweisgebersystem bei der Konzernmutter angesiedelt, besteht eine gemeinsame Verantwortlichkeit für den technischen Betrieb des Hinweisgebersystems. Innerhalb der Unternehmensgruppe muss daher eine entsprechende Vereinbarung nach Art. 26 DSGVO, ein „Joint Controller Agreement“ abgeschlossen werden.

Das vorliegende Gesetz geht auch auf das Spannungsverhältnis zwischen einerseits den Rechten der betroffenen Person nach der DSGVO und andererseits den Rechten des Hinweisgebers auf Vertraulichkeit ein. Solange es zum Zweck der Ermittlung und Verfolgung der in einem Hinweis vorgeworfenen Rechtsverletzung und des Hinweisgeberschutzgesetzes erforderlich ist, finden die Datenschutzrechte der vom Hinweis betroffenen Person (Recht auf Information, Recht auf Auskunft, Recht auf Berichtigung, Recht auf Löschung und Recht auf Einschränkung der Verarbeitung) keine Anwendung.

Welche Sanktionen drohen nach dem Hinweisgeber-schutzgesetz?

Verstöße gegen die wesentlichen Vorgaben des Gesetzes wie zum Beispiel die Behinderung der Hinweisgebung, die Ergreifung von Vergeltungsmaßnahmen, die Anstrengung mutwillig gerichtlicher oder verwaltungsbehördlicher Verfahren, die Verletzung des Schutzes

der Identität des Hinweisgebers sowie wissentlich falsche oder irreführende Hinweise von Hinweisgebern werden mit einer Verwaltungsstrafe von bis zu 20.000 Euro, im Wiederholungsfall bis zu 40.000 Euro bestraft.