HINWEISGEBERSCHUTZGESETZ

MEHR SICHERHEIT FÜR WHISTLEBLOWER

2023 stehen Unternehmen vor neuen Aufgaben: Das geplante Hinweisgeberschutzgesetz sieht vor, dass Firmen eine neutrale Meldestelle einrichten. Mitarbeiter haben so die Chance, auf Rechtsverstöße zu verweisen, ohne Nachteile befürchten zu müssen. Die neue Pflicht gilt für Betriebe ab 50 Mitarbeitern. Auch kleinere Systeme profitieren von einem internen Anlaufpunkt. Wer die Vorgaben ignoriert, dem drohen Bußgelder.

© Danijel Grbic Bebop Media

Achim Barth

Die neue Hinweisgeberschutzrichtlinie fordert ein neutrales Meldesystem für Rechtsverstöße. Genauer: Der aktuelle Entwurf verlangt, dass Organisationen eine unabhängige Anlaufstelle einrichten, über die Mitarbeiter Verfehlungen gegen Compliance-Regeln, deutsches Recht oder EU-Recht melden können. Das System hat zwei Hauptanliegen: Zum einen soll es Angestellten erleichtern, einen kritischen Vorfall innerhalb ihres Betriebes vorzubringen – als Hinweisgeber gelten alle Beschäftigen eines Unternehmens oder einer Behörde, vom Festangestellten bis zum Freiberufler. Gleichzeitig soll das Gesetz die meldenden Kollegen vor Repressalien verschonen. Bisher waren Informanten nicht vor Abmahnungen, Kündigungen oder anderweitigen Schikanen geschützt.

Dass die Richtlinie kommt, steht außer Frage. Bereits 2019 trat die EU-Whistleblower-Richtlinie in Kraft. Weder zivilrechtlich, strafrechtlich, verwaltungsrechtlich noch arbeitsrechtlich dürfen Beschäftigte seitdem für Warnungen haftbar gemacht werden. Bis Ende 2021 sollte Deutschland die europäische Variante in nationales Recht umsetzen. Die Frist ist verstrichen. Wegen der Verzögerung startete die EU bereits ein Vertragsverletzungsverfahren gegen Deutschland. Mit dem taufrischen Hinweisgeberschutzgesetz (HinSchG) steht die verspätete Antwort nun in den Startlöchern – und deutsche Unternehmen vor neuen Aufgaben.

Sobald das Gesetz beschlossen ist, drängt die Zeit. Dann haben Organisationen mit mehr als 250 Angestellten drei Monate Zeit, die Anforderungen zu erfüllen. Für Unternehmen ab 50 Mitarbeitern gilt das neue Gesetz ab Dezember 2023. Wer die Vorgaben ignoriert, muss mit einem Bußgeld von 20.000 € rechnen. Ähnlich wie beim Start der Datenschutzgrundverordnung 2018 könnte das neue deutsche Whistleblowergesetz für große Unruhe sorgen. Die Fragen der Führungskräfte klingen wie damals: Was genau verlangt das Papier? Was gilt es umzusetzen? Worum geht es technisch? Wer darf Meldungen annehmen? Und welche Fristen gelten für wen?

Sobald das Gesetz beschlossen ist, drängt die Zeit.

Neutrale Anlaufstelle ermöglicht, Sachverhalte intern zu prüfen

Die neue Norm soll Arbeitnehmer schützen. Jedoch profitieren Unternehmen ebenso von einer internen Anlaufstelle für Whistleblower. Wer keine bewussten Verstöße begeht, hat sowieso nichts zu befürchten. Wer unwissentlich Gesetze missachtet, kann das Ganze als Frühwarnsystem betrachten. Da Beschäftigte Missstände in den eigenen Firmenwänden oft als erste wahrnehmen, können sie unentdeckte Rechtsverstöße leichter ans Licht bringen. Experten haben so die Chance, den Sachverhalt intern zu prüfen, zu verfolgen und abzustellen, bevor die Information an die Öffentlichkeit gelangt. Deshalb lohnt sich eine solche Zentrale ebenso für KMU unter 50 Mitarbeitenden. Schließlich kann jeder Informant frei entscheiden: Verkündet er den Verstoß bei der hauseigenen Meldestelle? Oder alarmiert er eine der drei externen Anlaufpunkte des Bundes (Bundesministerium für Justiz, Bundesanstalt für Finanzdienstleistungen, Bundeskartellamt)?

© Danijel Grbic Bebop Media

Wendet sich ein Kollege direkt an eine Bundesstelle, ordnet diese mit hoher Wahrscheinlichkeit eine staatliche Prüfung an. Das nagt am Firmenimage. Der Ruf leidet massiv, wenn externe Ermittler den Betrieb unter die Lupe nehmen. Wer vermeiden will, das Andeutungen auf Umweltverstöße, Hygienemängel oder der Verdacht auf Straftaten wie Steuerhinterziehung oder Datenmissbrauch an die Öffentlichkeit gelangen, richtet ein möglichst attraktives und einfach zu bedienendes internes System ein – zumal bei Verhinderung ein Bußgeld von bis zu 100.000 € droht. Ein komfortabler Kanal senkt die Wahrscheinlichkeit, dass Mitarbeiter sich bei staatlichen Stellen beschweren. Durch frühzeitiges Eingreifen lassen sich zudem Haftungsansprüche und Reputationsschäden vermeiden.

Der Ruf leidet massiv, wenn externe Ermittler den Betrieb unter die Lupe nehmen.

Ein reiner „Kummerkasten“ reicht nicht aus

Jeder Mitarbeiter muss die Möglichkeit haben, Verstöße ohne Umwege mündlich oder schriftlich zu Gehör zu bringen. Die Unternehmen verpflichten sich, eine vertrauliche bis vollständig anonyme Kommunikation zwischen Hinweisgeber und Meldestelle zu garantieren. Nur ein elektronischer Kanal wird diesen Anforderungen gerecht. Ein reiner „Kummerkasten“, eine E-Mail-Adresse oder eine Telefonhotline reichen kaum aus. Ein E-Mail-Postfach garantiert nicht automatisch Vertraulichkeit. Administratoren könnten Zugriff haben, oder jemand versendet Dokumente mit personenbezogenen Metadaten. Über einen softwaregestützten Kanal lassen sich Fristen optimal verwalten, der Austausch bleibt vertraulich, beide Seiten können Dokumente hochladen, und der Kommunikationsverlauf lässt sich ideal dokumentieren.

Die Vorschrift sieht vor, dass Organisationen neben solch einem Kanal einen Meldestellenbeauftragten benennen. Wie beim Datenschutzbeauftragten gilt hier: Diese Person muss unabhängig, weisungsungebunden und frei von Interessenkonflikten arbeiten. Diese Funktion kann somit weder jemand aus der Personalabteilung noch ein Betriebsratsmitglied oder der betriebliche Datenschutzbeauftragte übernehmen. Gleichzeitig braucht der Kandidat Fachkenntnis. Er muss sich in die Materie einarbeiten und regelmäßig weiterbilden. Einen Mitarbeiter bringt das schnell an seine Belastungsgrenzen.

Die Vorschrift sieht vor, dass Organisationen neben solch einem Kanal einen Meldestellenbeauftragten benennen.

Hilfe von Profis: Wissen über Technik und Rechtslage

Um die Anforderungen zu erfüllen und das Ganze effizient zu gestalten, empfiehlt es sich, einen externen Dienstleister als Meldestelle zu benennen. Dieser sollte gleichzeitig den elektronischen Kanal zur Verfügung stellen. Infrage kommen zum Beispiel ein neutraler Ombudsmann bei einer Anwaltskanzlei oder ein externer Datenschutzbeauftragter. Solche Experten verfügen über den aktuellen Wissensstand zu Technik und Rechtslage. Außerdem sind sie versiert darin, Auskünfte vertrauensvoll entgegenzunehmen, sachlich zu bewerten und mit den Beteiligten angemessen zu kommunizieren.

Sobald die technische Anlaufstelle eingerichtet ist, sollte jemand die Teams über die Vorgehensweise aufklären. Erfahrene interne oder externe Fachleute informieren die Kollegen zeitnah. Am besten eignet sich eine Compliance-Schulung, in der der Meldestellenbeauftragte das Wesen des internen Knotenpunkts und die neuen Möglichkeiten erläutert. Es ist zudem sinnvoll, die Teams über eine Richtlinie oder Betriebsvereinbarung in den Prozess einzubinden. Führungskräfte sollten sich gesondert darin schulen, wie sie mit Hinweisgebern umgehen, die sich direkt an sie wenden.

Sobald die technische Anlaufstelle eingerichtet ist, sollte jemand die Teams über die Vorgehensweise aufklären.

Ein Verdacht nimmt seinen Weg

Bei Eingang einer Nachricht erhält der Hinweisgeber innerhalb von sieben Tagen eine Eingangsbestätigung. Der Fall wird dokumentiert und revisionssicher erfasst. Dann beginnt die Untersuchung. Die Meldestelle prüft den Vorfall unvoreingenommen, spricht mit Betroffenen und Hinweisgebern und verweist gegebenenfalls

© WrightStudio - stock.adobe.com

an andere zuständige Stellen. Dafür hat die beauftragte Vertrauensperson drei Monate Zeit. In dieser Zeit hält sie den Informanten über die bereits ergriffenen oder geplanten Maßnahmen auf dem Laufenden und begründet ihr jeweiliges Vorgehen. Wird nichts unternommen, können die Beschäftigten jederzeit staatliche Stellen und die Öffentlichkeit informieren.

Gleichzeitig ist der Unternehmer der neuen Richtlinie nicht schutzlos ausgeliefert: Geht eine Falschmeldung ein und entsteht dadurch ein Schaden, muss der Angestellte dafür aufkommen. Dies ist besonders wichtig, da das Melderecht die Umgehung von Verschwiegenheits- oder Geheimhaltungspflichten erlaubt. Um auf der sicheren Seite zu sein, empfiehlt es sich erneut, externe Profis mit ins Boot zu holen: Wer die Sache einem Partner überlässt, spart viel Zeit und Nerven, die er sonst in den Aufbau und die Pflege des neuen Hinweisgebersystems investieren müsste.

Über den Autor

Wie zähmt man das Bürokratie-Monster DSGVO? Achim Barth ist einer der kompetentesten Ansprechpartner rund um den Schutz personenbezogener Daten. In der Beratung, in Seminaren und Vorträgen überzeugt der Gründer von „Barth Datenschutz" mit praktikablen Lösungen.

BUCHTIPP

Achim Barth

Haltet den Datendieb!

Wer Ihre Daten will. Was er damit treibt. Wie Sie sich schützen.

GABAL Verlag, Offenbach
224 Seiten
ISBN 978-3-96739-130-5
€ 24,90

Erscheinungstermin: 28. März 2023

Jede Minute hinterlassen wir Unmengen an Spuren im Netz – wir suchen eine Adresse bei Google Maps, wir schreiben über WhatsApp, ein Freund markiert uns im Foto, wir retweeten einen Beitrag … Wir wissen alle, dass wir zu viele Daten hinterlassen. Doch es ist unmöglich geworden, sich im Alltag ohne Smartphone und Apps zurechtzufinden. Schnell schleicht sich Resignation ein. Nach der Lektüre von „Haltet den Datendieb!" werden Sie Ihr Verhalten kritischer sehen. Lernen Sie, was Datensammler und Datenräuber mit Ihren Daten wirklich treiben und welche Gefahren auch in Zukunft auf uns lauern. Erfahren Sie, wie Sie sich wappnen können, um Ihre digitale Privatsphäre zu schützen. Werfen Sie weniger digitale Schatten, bewahren Sie Ihr Grundrecht auf informationelle Selbstbestimmung und bauen Sie die Kompetenzen für den sicheren Umgang mit modernen Technologien auf. *ab*