Neue „Whistleblower-Richtlinie“ nimmt Unternehmen in die Pflicht

Meldesysteme. Rechtsanwalt Fabian Bösch von der Kanzlei Greiter, Pegger, Kofler & Partner zeigt auf, welche Auswirkungen die EU-Richtlinie 2019/1937 auf die Wirtschaft hat.

© freshidea - stock.adobe.com

Die EU-Richtlinie 2019/1937 zielt nicht zuletzt darauf ab, sogenannte Whistleblower, die Missstände aufzeigen wollen, unter Schutz zu stellen.

Spätestens seit Edward Snowden und WikiLeaks ist das Thema Whistleblowing jedem ein Begriff. Allgemein gesprochen versteht man darunter das Aufdecken von Missständen in Unternehmen und Behörden. Eine neue EU-Richtlinie sieht vor, dass in den Mitgliedstaaten ab Jahresende viele Unternehmen verpflichtet sein werden, ein Whistleblowing-System einzuführen.

Derzeitige Situation: Whistleblowing-Systeme sollen es Mitarbeitern ermöglichen, unternehmens- oder behördenin-terne Missstände an die Führungsebene heranzutragen, ohne Nachteile für sich selbst – etwa durch Kündigung, Versetzung etc. – befürchten zu müssen.

Derzeit werden solche Systeme nur vereinzelt und insbesondere bei Behörden wie der Wirtschafts- und Korruptionsstaatsanwaltschaft, der Bundeswettbewerbsbehörde oder der Finanzmarktaufsicht eingesetzt. Aber auch einige Unternehmen haben derartige Systeme, insbesondere zur Erlangung von Zertifizierungen nach ISO 19600 (Compliance Management Systeme) und ISO 37001 (Anti-Korruptionsmanagement-Systeme), bereits umgesetzt.

Für Kreditinstitute sieht das Bankwesengesetz schon jetzt eine Pflicht zur Einrichtung eines Whistleblowing-Systems vor.

Whistleblowing-Richtlinie

Am 16. Dezember 2019 trat die Richtlinie (EU) 2019/1937 („Whistleblowing-Richtlinie“) in Kraft. Sie sieht für bestimmte Unternehmen und Behörden künftig verpflichtende Meldekanäle vor. Dabei werden unter anderem Vorgaben zur konkreten Ausgestaltung dieser Kanäle (Whistleblowing-Systeme), zu Informations- und Dokumentationspflichten, zum Schutz der Whistleblower sowie zum Umgang mit personenbezogenen Daten festgelegt. Darüber hinaus regelt die Richtlinie auch Sanktionen für allfällige Verstöße gegen die Schutzpflichten durch Unternehmen und Behörden.

Whistleblower sind vor Repressalien durch das Unternehmen wie Suspendierungen, Entlassungen, Gehaltseinbußen, Diskriminierung oder Ähnlichem zu schützen. Es dürfen auch keine Verfahren wegen Verleumdung, Urheberrechtsverletzungen oder der Offenlegung von Geschäftsgeheimnissen eingeleitet werden. Hierbei gilt sogar eine Beweislastumkehr zu Lasten des Unternehmens. Dieses muss im Streitfall nachweisen, dass es keine Vergeltungsmaßnahmen wegen einer vom Schutz umfassten Meldung gesetzt hat.

In den Genuss des vorgenannten Schutzes kommen Whistleblower aber nur dann, wenn im Zeitpunkt der Meldung ein hinreichender Grund zur Annahme bestand, dass die gemeldete Information wahr ist. Bei mutwilligen oder gar bewusst falschen Meldungen besteht kein Schutzanspruch.

Darüber hinaus müssen sich Whistleblower grundsätzlich an ein dreistufiges Meldesystem halten. Zunächst ist eine Meldung über das Whistleblowing-System des Unternehmens (interne Meldung) vorzunehmen. Fruchtet das nicht, kann sich der Whistleblower an die zuständige Behörde (externe Meldung) wenden. Überspringt der Whistleblower das interne Meldesystem und wendet sich gleich an die Behörde, so bleibt er dennoch geschützt. Medien und andere Formen der Öffentlichkeit dürfen aber bei sonstigem Verlust des Schutzes erst dann eingeschaltet werden, wenn auch die externe Meldung keine Abhilfe schaffen konnte oder diese von vornherein aussichtslos war (z.B. wegen Aussichtslosigkeit, einer Notsituation oder Verstößen durch die Behörde selbst).

Das einzurichtende Whistleblowing-System muss unter anderem folgenden Anforderungen genügen:

- Leicht zugängliche Informationen über interne und externe Meldestellen (Behörden) und über die Voraussetzungen zur Inanspruchnahme der Schutzbestimmungen
- Ernennung einer zur Untersuchung von Hinweisen zuständigen Stelle
- Vertrauliche (nicht zwingend anonyme) Behandlung der Identität des Whistleblowers
- Rückmeldung an den Whistleblower binnen sieben Tagen über Eingang der Meldung und binnen drei Monaten über ergriffene Maßnahmen
- Dokumentation jeder Meldung

Eine allgemeine Pflicht für Mitarbeiter, jegliche bekanntgewordenen Verstöße dem Unternehmen zu melden, sieht die Richtlinie nicht vor.

Die Richtlinie ist als solche in den EU-Mitgliedstaaten nicht direkt anwendbar, sondern bedarf einer nationalen Umsetzung durch deren Parlamente, die längstens bis 17. Dezember 2021 zu erfolgen hat. Lediglich die Pflicht zur Einrichtung von Whistleblowing-Systemen bei Unternehmen mit weniger als 250 Mitarbeitern muss erst bis 17. Dezember 2023 in Kraft treten. Hier haben die nationalen Gesetzgeber also etwas mehr zeitlichen Spielraum. In Österreich liegt bis dato noch kein Entwurf zur Umsetzung vor.

Betrachtet man den laufenden Anpassungsbedarf bei den COVID-Bestimmungen, der dem öster-reichischen Gesetzgeber derzeit wenig Zeit für anderes lässt, ist zu befürchten, dass die nationale Umsetzung der Whistleblowing-Richtlinie erst kurz vor Ablauf der Frist am 17. Dezember 2021 erfolgen könnte. Es erscheint daher sinnvoll, sich bereits jetzt Gedanken über dieses Thema zu machen und erste Vorbereitungen zu treffen.

Die Implementierung und Betreibung eines Whistleblowing-Systems kostet naturgemäß Zeit und Geld. Es liegt daher die Versuchung nahe, sich für das günstigste und für das Unternehmen ein-fachste Whistleblowing-System zu entscheiden und sich bei der Umsetzung auf die gesetzlichen Mindestanforderungen zu beschränken.

Im Hinblick darauf, dass potenzielle Whistleblower auch dann geschützt sind, wenn sie sich gleich an die zuständigen Behörden wenden, sollte dennoch ein möglichst praktisches System mit niedri-ger Hemmschwelle eingeführt werden. Denn so unangenehm Whistleblower für ein Unternehmen auch sein können – noch viel unangenehmer wäre es, wenn das Unternehmen Missstände erst im Rahmen von behördlichen Ermittlungen oder Zeitungsberichten erfahren würde. ▲

Umsetzung im Unternehmen

Die Richtlinie verpflichtet alle Unternehmen ab einer Mindestzahl von 50 Mitarbeitern zur Einrichtung von Whistleblowing-Systemen, mit denen die Verletzung von EU-Recht (z.B. Umweltschutz, Datenschutz, Kartellrecht, Verbraucherschutz etc.) und – je nach nationaler Umsetzung – allenfalls nationalen Vorschriften angezeigt werden können.

Ist die Richtlinie anwendbar, muss sich das Unternehmen zu Beginn überlegen, wie und wo Meldungen eingebracht werden sollen (mündlich oder schriftlich, digital oder analog, interne Meldestelle oder externe Ombudsperson), wer die Meldungen bearbeitet und wer über allfällige weitere Maßnahmen entscheidet.

Da die Einführung eines Whistleblowing-Systems im Regelfall eine die Menschenwürde berührende Kontrollmaßnahme oder zumindest eine automationsunterstützte Personaldatenverarbeitung darstellen wird, ist meist die Mitwirkung des Betriebsrats erforderlich.

Darüber hinaus sollte auch ein allenfalls bestellter Datenschutzbeauftragter oder die sonstige für Datenschutzfragen zuständige Ansprechperson frühzeitig eingebunden werden.

Hat sich das Unternehmen für ein bestimmtes System entschieden, müssen die Arbeitnehmer darüber entsprechend informiert werden (Infobroschüren, Schulungen, Leitfaden im Intranet etc.).

Im Wesentlichen sollte ein Unternehmen also die folgenden Schritte umsetzen:

- Prüfung, ob das Unternehmen in den Anwendungsbereich fällt
- Festlegung der Anforderungen an das Whistleblowing-System (Für wie viele Mitarbeiter? Wie viele Standorte? Auch international? Geeignetes Personal für die Bearbeitung der Meldungen vorhanden?)
- Entscheidung für ein System
- Erstellung eines Umsetzungsplans
- Abstimmung mit dem Betriebsrat
- Abstimmung mit dem Ansprechpartner für Datenschutz
- Abschluss einer Betriebsvereinbarung
- Berücksichtigung in der Datenschutzdokumentation (z.B. Update Verfahrensverzeichnis, Datenschutzfolgenabschätzung)
- Erstellung und Verteilung der Unterlagen zur Mitarbeiterinformation
- Schulung der Führungskräfte und Ansprechpersonen für Meldungen
- Aktivierung des Whistleblowing-Systems
- Wiederkehrende Evaluierung

© Julia Türtscher, BLICKFANG

Zum Autor:
Mag. Fabian Bösch, B.A. ist Rechtsanwalt und Partner in der Kanzlei Greiter Pegger Kofler & Partner (www.lawfirm.at). Seine Tätigkeitsschwerpunkte liegen im Arbeits- und Datenschutzrecht sowie in den Bereichen Digitalisierung, IP- und IT-Recht. Er ist außerdem auch zertifizierter Datenschutzbeauftragter (TÜV).