

Interview: Hinweisgeberschutz – Umsetzung der EU-RL durch Gesetzgeber und Unternehmen

# „Ohne ein Hinweisgebersystem besteht die Gefahr, dass Risiken nicht erkannt werden“

Der Deutsche Bundestag hat am 16.12.2022 nach langem Warten das nationale Hinweisgeberschutzgesetz verabschiedet, mit dem die EU-Whistleblower-Richtlinie (EU-Richtlinie 2019/1937) umgesetzt werden soll. Wie ist das Gesetz zu bewerten? Über die Hintergründe, Whistleblower-Systeme, deren Nutzen und Risiken für Unternehmen sowie Best-Practice-Lösungen haben wir mit Marcus Sultzer, Vorstandsmitglied der EQS Group AG, gesprochen.

**Marcus Sultzer**  
Diplom-Betriebswirt und als  
Vorstandsmitglied der EQS  
Group AG verantwortlich für die  
globalen Umsätze, Marketing  
sowie Produkte und  
Partnerschaften



© EQS Group AG

**Edward Snowden, Julian Assange, Chelsea Manning ... keiner dieser Fälle betrifft deutsche Unternehmen. Wie groß ist die praktische Bedeutung des Hinweisgeberschutzes hierzulande überhaupt?**

Es ist richtig, nur die wenigsten Whistleblower erlangen eine Berühmtheit wie die drei Genannten, die mit ihren Enthüllungen weltweit für Schlagzeilen sorgten. In der Regel sind die Fälle nicht so spektakulär und weit weniger öffentlichkeitswirksam: Die Pflegerin, die menschenunwürdige Zustände im Altenheim aufdeckt, oder der Betriebswirt, der auf Betrügereien im Betrieb gestoßen ist, sind häufig nur eine Randnotiz in den Medien. Bei einem umfassenden Schutz der Hinweisgebenden wären Skandale wie Cum-Ex, die Panama Papers, Wirecard oder die Corona-Maskendeals vielleicht früher entdeckt und damit teilweise milliardenschwere Schäden verhindert worden.

**Ausgangspunkt des deutschen Hinweisgeberschutzgesetzes ist die EU-Hinweisgeberrichtlinie. Was sieht diese vor?**

**Was sind die Hintergründe und Ziele?**

Der offizielle Name der EU-Hinweisgeberrichtlinie, die im Dezember 2019 in Kraft trat, ist ein wenig sperrig: „Richtlinie des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“. Die Botschaft dahinter ist jedoch eindeutig: Unternehmen sind in der Pflicht, Maßnahmen zu ergreifen, um den Mitarbeitenden, aber auch externen Anspruchsgruppen wie Lieferanten oder Kunden die Möglichkeit zu geben, auf unethische oder illegale Verhaltensweisen wie Steuerbetrug, Geldwäsche oder Datenschutzverletzungen hinzuweisen – ohne Sanktionen bis zur Entlassung oder andere Repressalien befürchten zu müssen. Im ersten Schritt gilt das Gesetz für Unternehmen ab 250 Beschäftigten.

**Herr Sultzer, zunächst die ganz grundlegende Frage: Was ist ein Hinweisgeber?**

Hinweisgeber, vielen besser als Whistleblower bekannt, sind Personen, die auf unethisches oder illegales Verhalten in Unternehmen, Behörden oder anderen Organisationen hinweisen. Meldungen von Whistleblowern haben schon häufig Ermittlungen ins Rollen gebracht, an deren Ende große Skandale aufgedeckt werden konnten.

**In Deutschland hatten Whistleblower lange Zeit einen schlechten Ruf. Woher kommt das und hat es sich mittlerweile gewandelt?**

Leider ist das Ansehen von Whistleblowern in der Öffentlichkeit immer noch nicht so, wie es wünschenswert wäre. Es ist in der Tat traurig, dass diese immer noch befürchten müssen, dass ihre Glaubwürdigkeit angezweifelt wird und sie als Nestbeschmutzer oder Denunzianten abgestempelt werden. Häufig werden sie unter Druck gesetzt, schikaniert und erhalten nicht selten sogar die Kündigung. Deshalb ist es höchste Zeit, hier mit einem umfassenden Hinweisgeberschutz für Rechtssicherheit zu sorgen. Das wäre ein wichtiger Beitrag für mehr Integrität in der Wirtschaft.

### Das deutsche Umsetzungsgesetz hat lange auf sich warten lassen. Wie ist der aktuelle Stand?

Hier ist vor Weihnachten noch einmal viel Bewegung in die Angelegenheit gekommen. Der Deutsche Bundestag hat in seiner letzten Sitzung des Jahres das Hinweisgeberschutzgesetz verabschiedet. Jetzt muss es noch vom Bundesrat abgesegnet werden.

Das Gesetz, da stimme ich Ihnen zu, hat tatsächlich einen langen Anlauf genommen. Bereits Ende 2020 legte Christine Lambrecht, Bundesjustizministerin der Großen Koalition, den Entwurf eines „Gesetzes für einen besseren Schutz hinweisgebender Personen“ vor – scheiterte aber am Widerstand des Koalitionspartners CDU/CSU, dem die Regelungen zu weit gingen. Damit blieb das Thema für die aktuelle Ampelkoalition liegen.

### Was genau sieht das Gesetz vor?

Das Hinweisgeberschutzgesetz kommt zwar mit gut einem Jahr Verspätung, doch diese Zeit wurde sinnvoll genutzt. Aus unserer Sicht ist besonders erfreulich, dass beim Schutz der Whistleblower nochmals nachgebessert wurde: Meldestellen müssen nun auch anonymen Hinweisen nachgehen und Vorkehrungen treffen, um eine anonyme Kommunikation mit den meldenden Personen zu ermöglichen. Im letzten Regierungsentwurf war diesbezüglich nur eine Empfehlung – „sollen sich beschäftigen“ – ausgesprochen worden, im ersten Entwurf gab es überhaupt keine Pflicht, Hinweisen ohne Angaben zur Identität nachzugehen. Der Verzicht auf anonyme Meldungen hätte sowohl für die meldenden Personen als auch für Unternehmen ein unkalkulierbares Risiko bedeutet. Es ist daher wichtig und richtig, dass hier nochmals nachgebessert wurde, denn ohne den Schutz der Identität der meldenden Personen erreichen viele wertvolle Hinweise die Unternehmen nicht oder nur mit erheblicher Verzögerung.

Laut dem „Whistleblowing Report 2021“, einer internationalen Studie der Fachhochschule Graubünden, die auch im Entwurf des deutschen Hinweisgeberschutzgesetzes mehrfach als Quelle genannt wird, ging im Jahr 2020 jeder zweite Hinweis ohne Angaben zur Person bei den Unternehmen ein. Deshalb wurde bspw. auch von der Antikorruptionsorganisation Transparency Deutschland kritisiert, dass der erste Entwurf der Ampelkoalition weder eine Pflicht beinhaltete, anonyme Meldungen zuzulassen, noch diesen Hinweisen nachzugehen.

### Wie ist darüber hinaus der Inhalt zu bewerten?

Hier sehen wir einen wirklich positiven Aspekt. Beim Anwendungsbereich geht das Gesetz über die Anforderungen der EU-Richtlinie und auch den letzten Regierungsentwurf hinaus und beschränkt sich nicht nur auf das Unionsrecht. Unter bestimmten Voraussetzungen werden auch Meldungen von Verstößen gegen nationales Recht erfasst. Das betrifft einerseits Straftaten und andererseits Bußgeldtatbestände, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient.

Unter den „sonstigen Verstößen“, die das Gesetz in Zukunft abdecken soll, werden u. a. Geldwäsche und Steuerbetrug, aber auch Verstöße gegen Vorgaben zum Umweltschutz oder zur Lebensmittelsicherheit genannt. Das sorgt auch für Rechtssicherheit, denn ansonsten hätten sich hinweisgebende Personen immer erst absichern müssen, ob sie zu EU-Recht melden und damit den Schutz des Gesetzes genießen.

### Wie haben andere EU-Staaten die Richtlinie umgesetzt?

Auch hier hat sich zuletzt viel getan. Anfang Dezember, also fast zwölf Monate nachdem die Pflicht zur Umsetzung der EU-Richtlinie abgelaufen ist, verfügte erst gut ein Drittel der EU-Staaten über ein nationales Hinweisgeberschutzgesetz. Dann brachten neben Deutschland auch Belgien und Italien ihre nationalen Hinweisgeberschutzgesetze auf den Weg. Vorbildlich war hier vor allem Dänemark, dessen Gesetz bereits im Sommer 2021 verabschiedet wurde. Inhaltlich gehen die Dänen wie Deutschland, aber bspw. auch Schweden und Frankreich über die Anforderungen der EU-Richtlinie hinaus. Damit werden in Kürze von den fünf EU-Staaten mit den meisten Einwohnern neben Frankreich auch Deutschland und Italien ihre Hinweisgeber durch ein nationales Gesetz schützen. Gegen die Länder, die noch keinen Vollzug gemeldet haben, hatte die EU-Kommission bereits ein förmliches Vertragsverletzungsverfahren eingeleitet.

### Wie funktionieren Whistleblower-Systeme? Welchen Nutzen haben sie für Unternehmen?

Ein digitales Hinweisgebersystem ist ein effizientes Frühwarnsystem für Unternehmen, um Risiken frühzeitig zu erkennen und Schaden vom Unternehmen abzuwenden. Mitarbeitende oder externe Anspruchsgruppen wie Kunden, Geschäftspartner oder Lieferanten können über das Tool Hinweise auf rechtliche oder ethische Verstöße anonym und verschlüsselt abgeben. Das System ermöglicht außerdem eine geschützte Kommunikation mit den Personen, die Missstände gemeldet haben. Jeder Schritt des Verfahrens wird DSGVO-konform und revisions sicher dokumentiert.

### Wo liegen die Grenzen? Welche Maßnahmen können Unternehmen ergreifen, wenn diese erreicht sind?

Jedes System ist nur so gut wie die Compliance-Kultur, die im jeweiligen Unternehmen vorherrscht – das muss jedem klar sein. Es ist also wichtig, dass Werte und ethische Grundsätze klar kommuniziert und vom Management vorgelebt werden. Stichwort: „Tone from the Top“. Außerdem braucht es eine klar definierte Compliance-Organisation, die die Zuständigkeiten bei Hinweisen auf Missstände regelt und die sich daraus ergebenden Prozesse und Eskalationsprinzipien vorgibt. Hier muss der Vorstand bzw. die Geschäftsführung die entsprechenden Strukturen schaffen. Um Gefahren für das Unternehmen frühzeitig zu erkennen und wirkungsvolle Präventions- und Abhilfemaßnahmen ergreifen zu können,

empfiehlt es sich außerdem, ein effizientes Risikomanagement zu etablieren.

### Welche Vor- und Nachteile haben digitale Lösungen gegenüber persönlichen Meldewegen?

Wir sehen eigentlich keine Nachteile digitaler Lösungen, denn diese erleichtern mit ihren intelligenten und intuitiven Workflows die tägliche Arbeit der Compliance-Verantwortlichen erheblich.

Unternehmen, die auf automatisierte Arbeitsabläufe setzen, sparen zudem Zeit und Geld. Es ist deshalb nicht verwunderlich, dass die webbasierten Lösungen sich in den letzten 20 Jahren bewährt und als Best Practice etabliert haben, denn nur sie erfüllen alle Anforderungen an eine sichere, anonyme und DSGVO-konforme Kommunikation. Andere Meldewege können dies alles gar nicht gewährleisten. Eine Telefonhotline, ein E-Mail-Postfach oder ein spezieller Briefkasten für Hinweise, die Unternehmen theoretisch auch einrichten könnten, erfüllen allenfalls Mindeststandards – die von Experten dringend eingeforderte Wahrung der Anonymität der meldenden Personen kann mit diesen Lösungen jedoch nicht sichergestellt werden. Die Hinweisgebenden könnten, wenn es hart auf hart kommt, über die Stimme, Schrift oder IP-Adresse identifiziert werden.

### Wie wird die Anonymität der Hinweisgebenden Person gewährleistet?

Digitale Systeme sind der einzige sichere Weg für Hinweisgebende, um Missstände wie Korruption, Amtsmissbrauch, Diskriminierung oder Belästigung sowie Verstöße gegen interne Richtlinien zu melden. Die Kommunikation ist verschlüsselt, damit können die meldenden Personen auch nach ihrem Hinweis Rückfragen der Compliance-Beauftragten beantworten und weiter zur Aufklärung des Sachverhalts beitragen, ohne ihre Identität preisgeben zu müssen. So wird die Hemmschwelle bei Mitarbeitenden oder externen Stakeholdern, die vor allem vor der ersten Meldung sehr hoch ist, deutlich herabgesetzt. Aus unserer langjährigen Erfahrung ist es außerdem zu empfehlen, dass die Abgabe der Hinweise in Landessprache möglich ist, damit Mitarbeitende nicht aufgrund einer Sprachbarriere davon abgehalten werden, Hinweise zu geben. Es ist vor allem für international agierende Konzerne wichtig, verschiedene Sprachschienen anzubieten. Dies ist technisch ohne Weiteres möglich.

### Welche Möglichkeiten haben Whistleblower, um auf Missstände in ihrem Unternehmen aufmerksam zu machen? Können sie sich ohne Weiteres an die Öffentlichkeit wenden?

Die EU-Hinweisgeberrichtlinie und alle darauf fußenden nationalen Gesetze sehen drei Möglichkeiten vor, wie hinweisgebende Personen bei ihrer Meldung vorgehen können. Grundsätzlich haben sie Wahlfreiheit, ob sie den Verdacht oder Missstand intern beim eigenen Unternehmen melden möchten oder extern bei der zuständigen Aufsichtsbehörde. Als Ultima Ratio, wenn Hinweisgebende bei beiden Stellen kein Gehör finden, können sie sich auch an die

Öffentlichkeit wenden – und genießen denselben Schutz. Das deutsche Hinweisgeberschutzgesetz – und auch das ist neu – räumt internen Meldestellen Vorrang ein. Es appelliert an die Unternehmen, Anreize für die Nutzung der internen Meldeverfahren zu schaffen, ohne die Abgabe von Meldungen an die externe Stelle zu behindern.

### Wie ist das aus Unternehmenssicht zu bewerten?

Auf jeden Fall positiv. Sowohl das Melden an externe Behörden als auch an die Öffentlichkeit ist für Unternehmen in aller Regel die deutlich schlechtere Variante. Sie verlieren die Möglichkeit, Missstände proaktiv zu adressieren und riskieren signifikante Reputationsschäden sowie finanzielle Konsequenzen. Daher empfehlen wir allen Unternehmen, die interne Meldemöglichkeit so zugänglich wie möglich zu machen: mit der Option, anonym zu melden, in allen relevanten Sprachen, breit kommuniziert.

### Wie unterscheiden sich interne und externe Meldestellen?

Interne Meldestellen werden von unternehmens-eigenen Abteilungen oder Komitees betreut, z. B. Compliance, Internal Audit oder HR. Die Meldungen werden intern bearbeitet und bei relevanten Fällen interne Ermittlungen durchgeführt. Das funktioniert natürlich nur, wenn Unternehmen das Thema ernst nehmen – was im gegensätzlichen Fall passiert, hat uns das Beispiel Wirecard gezeigt. Externe Meldestellen sind in der Regel Behörden, in Deutschland allen voran das Bundesamt für Justiz, aber auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder das Bundeskartellamt. Laut dem Hinweisgeberschutzgesetz müssen Unternehmen darüber informieren, dass sich hinweisgebende Personen auch an diese Stellen wenden können. Hier können Unternehmen dann natürlich heikle Prozesse, Bußgelder und Reputationsschäden drohen.

### Wie erfolgen Meldungen in der Praxis und wie geht es danach weiter? Können Sie einmal den groben Ablauf schildern?

Ja, gern. Wenn eine Meldung eingegangen ist, versendet der Bearbeiter eine Eingangsbestätigung an die hinweisgebende Person, dies muss laut dem Gesetz innerhalb von sieben Tagen geschehen. Voraussetzung dafür ist, dass sie einen Postkasten für eine weiterführende Kommunikation eingerichtet hat – aufgrund der Verschlüsselung bleibt sie dabei natürlich, sofern gewünscht, weiter anonym. Es folgt eine Plausibilitätsprüfung, einige Unternehmen haben auch einen Compliance-Ausschuss, in dem die Meldungen und das weitere Vorgehen besprochen werden. Über die integrierte Meldungsbearbeitung können dann auch andere Abteilungen wie HR, Controlling oder Datenschutz in die Bearbeitung und Aufklärung der Sachverhalte einbezogen werden. Über den Postkasten, sofern vorhanden, werden dann häufig auch Rückfragen an die Hinweisgebenden gestellt. Nach spätestens drei Monaten sollen die

Hinweisgebenden eine Rückmeldung zu den geplanten oder bereits ergriffenen Maßnahmen erhalten. Die Empfangsbestätigung und die Rückmeldung sind neue Anforderungen, die sich aber auch digital abbilden lassen. Unternehmen, die bereits vor längerer Zeit proaktiv ein Hinweisgebersystem eingeführt haben, sollten dieses daher diesbezüglich noch einmal auf den Prüfstand stellen.

### **Ein aktueller deutscher Fall ist der der mittlerweile abgelösten RBB-Intendantin Patricia Schlesinger. Bestehen Unterschiede zwischen Systemen, die im öffentlichen – der RBB ist ja Teil des öffentlich-rechtlichen Rundfunks – und solchen, die im privaten Sektor zum Einsatz kommen?**

Die wesentliche Funktionsweise ist gleich. Unterschiede gibt es regelmäßig bei den Themenschwerpunkten, zu denen Meldungen abgegeben werden – und der internen Bearbeitung. Im öffentlichen Sektor geht es häufig um Bestechung von Amtsträgern, Vergabeprozesse, Finanzbetrug; außerdem werden die Meldungen i. d. R. nur in einer oder zwei Sprachen abgegeben. Im privaten Sektor sind die möglichen Themen häufig vielfältiger und je nach internationaler Ausrichtung des Unternehmens auch aus aller Welt zu erwarten.

### **Manche Unternehmen befürchten sich häufige Falschmeldungen.**

#### **Wie wahrscheinlich sind diese wirklich?**

Diese Befürchtung hört man ziemlich häufig von Unternehmen und Organisationen, wenn es um anonyme Meldungen geht. Dabei bestätigt sich dieser Vorbehalt nicht, wenn man noch einmal einen Blick in den „Whistleblowing Report 2021“ wirft. Nur rund 10 % der eingegangenen Meldungen stuften deutsche Firmen als missbräuchlich ein. Dabei hatte die Möglichkeit, anonym zu bleiben, keinen Einfluss auf diesen Anteil. Dagegen wiesen 45 % der Meldungen auf einen Compliance-relevanten Missstand hin. Die übrigen knapp 45 % sind zwar aus Compliance-Sicht nicht relevant, deuteten aber auf andere interne Probleme hin. Bei den befragten Unternehmen aus Frankreich, Großbritannien und der Schweiz war der Anteil der Meldungen, die die Intention hatten, den Kollegen oder dem Unternehmen gezielt Schaden zuzufügen, sogar noch geringer.

### **Müssen Personen, von denen solche Falschmeldung ausgehen, Sanktionen fürchten? Was sieht das Gesetz für diesen Fall vor?**

Das deutsche Hinweisgeberschutzgesetz sagt ganz klar, dass hinweisgebende Personen bei Falschmeldungen zum Ersatz des Schadens verpflichtet sind. Voraussetzung: Die Meldung oder Offenlegung der unrichtigen Informationen geschah vorsätzlich oder grob fahrlässig. Personen, die Vorgänge falsch einschätzen und nach bestem Wissen und Gewissen handeln und melden, haben damit nichts zu befürchten.

### **Worauf müssen Unternehmen ab 2023 achten?**

Viele deutsche Unternehmen werden ab 2023 direkt doppelt regulatorisch verpflichtet, interne Meldesysteme einzurichten: neben dem Hinweisgeberschutzgesetz auch durch das Lieferkettensorgfaltspflichtengesetz. Beide stellen spezifische Anforderungen an Unternehmen. So müssen bestimmte Rückmeldefristen eingehalten, jährliche Reports eingereicht und Informationen für Hinweisgebende in bestimmter Form vorgehalten werden, um nur einige Beispiele zu nennen.

### **Wie können und sollten Unternehmen sich jetzt vorbereiten?**

Der wichtigste Schritt ist, wie bereits erwähnt, eine ethische und starke Compliance-Kultur im Unternehmen zu etablieren. Das geht nicht von heute auf morgen, deshalb kann man gar nicht früh genug damit beginnen. Die Führungsebene sollte möglichst frühzeitig die entsprechenden Maßnahmen ergreifen und dabei auf Best Practice setzen. Dazu gehört auch ein Hinweisgebersystem, dessen erfolgreiche Implementierung stark von der Akzeptanz der Mitarbeitenden sowie von der klaren und transparenten Kommunikation der damit verbundenen Prozesse und Compliance-Maßnahmen abhängt. Und es gibt noch einen weiteren wichtigen Punkt, weshalb es empfehlenswert ist, rechtzeitig alles in die Wege zu leiten: Kleine Unternehmen mit mehr als 50 Beschäftigten haben zwar noch eine Schonfrist und müssen die geforderten internen Maßnahmen erst bis Ende des nächsten Jahres umsetzen. Allerdings können sich Personen, die Missstände oder Rechtsverstöße extern melden, bereits vorher auf den gesetzlichen Schutz berufen. Das heißt in der Praxis: Es besteht die Gefahr, dass sich Hinweisgebende an die Aufsichtsbehörden wenden, wenn kein interner Kanal zur Verfügung steht. Damit geben die Verantwortlichen das Heft des Handelns aus der Hand. Denn wenn die externen Untersuchungen erst einmal laufen, kann das Unternehmen nur noch reagieren. So weit sollte man es auf keinen Fall kommen lassen.

### **Was erwartet Arbeitgeber, die die Anforderungen des Gesetzes nicht erfüllen?**

Die Strafzahlungen von 20.000 Euro, die das Hinweisgeberschutzgesetz vorsieht, sind für die meisten Unternehmen nicht sonderlich abschreckend. Anders sieht das dagegen beim Lieferkettensorgfaltspflichtengesetz aus, das für das Beschwerdeverfahren ebenfalls ein Meldesystem verlangt, dessen Strafen in die Millionen gehen können. Hier drohen außerdem Schadensersatzklagen bei Verstößen gegen die Sorgfaltspflichten. Unternehmen sollten sich also schon aus Selbstschutz solide aufstellen, denn ohne ein Hinweisgebersystem besteht zudem die Gefahr, dass Risiken nicht erkannt werden. Neben dem daraus resultierenden finanziellen Schaden droht ein Reputationsverlust, der bei großen Verfehlungen kaum noch wettzumachen ist.

### **Vielen Dank für das Gespräch!**

Das Interview führte Anne Politz. ■