



WHISTLE- BLOWING

Rechtliche Hintergründe und
Tipps für die Praxis.

Aus der Broschürenserie **GUTE ARBEIT!**
Gewerkschaft GPA – Abteilung Arbeit & Technik

gpa
MEINE
GEWERKSCHAFT

IMPRESSUM:

Herausgeber: Gewerkschaft GPA, 1030 Wien, Alfred-Dallinger-Platz 1

Redaktion: Vera Erlachner, Gewerkschaft GPA – Abteilung Arbeit & Technik

Layout: Christina Schier, Gewerkschaft GPA – Abteilung Organisation und Marketing

Bilder/Fotos: AdobeStock, Konstantin Latsunas

ÖGB ZVR-Nr.: 576439352

Stand: März 2023



AUTORINNEN

Dr. Michael Gogola

ist Jurist und arbeitet in der Grundlagenabteilung sowie der Abteilung Arbeit & Technik der Gewerkschaft GPA. Er beschäftigt sich unter anderem mit den Themen Arbeitszeit, Digitalisierung und Datenschutz sowie mit Rechtsfragen der modernen Arbeitswelt.

Sebastian Klocker

ist Datenschutzexperte und arbeitet in der Abteilung Arbeit & Technik der Gewerkschaft GPA. Er beschäftigt sich vorrangig mit Beschäftigten-Datenschutz und IT-Security.

Unter Mitarbeit von:

Mag.^a Clara Fritsch

Mag.^a Claudia Kral-Bast

Die Inhalte sind nach bestem Wissen erstellt und sorgfältig geprüft. Es besteht jedoch keine Haftung seitens der AutorInnen oder der Gewerkschaft GPA. Inhalte dürfen unter Angabe der AutorInnen weiterverbreitet werden (CC-Urheberrecht).

Aus Gründen der Barrierefreiheit und Maschinenlesbarkeit wird in dieser Publikation das Binnen-I verwendet.

VORWORT



© Konstanin Latschias

Wer in die Trillerpfeife bläst (engl. Whistleblowing), sorgt für Aufmerksamkeit oder schlägt Alarm. WhistleblowerInnen decken Rechtsverletzungen oder andere gravierende Missstände in Betrieben und Organisationen auf und wollen, dass Missstände behandelt und aufgeklärt werden. Es geht ihnen darum, durch Informationsweitergabe an innerbetriebliche oder außerbetriebliche Stellen eine Veränderung in Gang zu setzen und rechtswidriges Verhalten abzustellen.

Solche Initiativen werden jedoch selten belohnt. Um diese risikoreiche Situation für WhistleblowerInnen zu entschärfen, um WhistleblowerInnen im Unternehmen zu bestärken, und um damit beizutragen, Missstände zu beseitigen, hat die Europäische Union 2019 eine Richtlinie "zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" erlassen.

Zumal das Thema von großer Relevanz für die betriebliche Praxis ist und dem Betriebsrat bei der Einführung eines HinweisgeberInnen-Systems eine wichtige Rolle zukommt, möchten wir mit der Neuauflage der Broschüre „Whistleblowing- Wenn ArbeitnehmerInnen Missstände aufdecken“ nicht länger warten.

Der vorliegende Arbeitsbehelf gibt einen thematischen Überblick, analysiert die rechtlichen Rahmenbedingungen, zeigt Spannungsfelder auf und gibt Tipps und Hilfestellung zur praktischen Umsetzung in den Betrieben.

Für weiterführende Information und Begleitung rund um betriebliche HinweisgeberInnen-Systeme steht die Gewerkschaft GPA gerne mit Rat und Tat zur Seite.

Verena Spitz

Vorsitzende des Beirats für Arbeit & Technik der Gewerkschaft GPA

INHALT

Whistleblowing	8
Whistleblowing – worum geht’s?	8
Whistleblowing – woher kommt’s?	9
Die europäische Whistleblowing-Richtlinie	12
Die Entstehung der der Whistleblowing-Richtlinie	12
Personen, die geschützt werden	12
Inhalte, die gemeldet werden	12
Verbotene Repressalien am Arbeitsplatz	13
Die Meldestelle	13
Pflicht, eine Meldestelle einzurichten	14
Externe Meldestelle	14
Gestaltung der Meldestelle	14
Fristen	15
Die österreichische Umsetzung der EU-Whistleblowing-Richtlinie	16
Das HinweisgeberInnenschutzgesetz	16
Der Betriebsrat und das Whistleblowing	18
Zusätzlicher Schutz des Betriebsratsmitglieds	18
Gesetzliche Grundlagen für die Betriebsvereinbarung (BV)	20
Whistleblowing und Arbeitsrecht	22
Keine generelle Meldepflicht	22
Die Treuepflicht begründet noch keine Verschwiegenheitspflicht	23
Whistleblowing und Geschäftsgeheimnis	24
Whistleblowing und Compliance/Verhaltensrichtlinien	24
Weitere Rechtsgrundlagen für Whistleblowing-Systeme	25

INHALT

Whistleblowing und Datenschutz	26
Information für ArbeitnehmerInnen	26
Datenschutz-Folgenabschätzung	26
Das Verarbeitungsverzeichnis	27
Die/der betriebliche Datenschutzbeauftragte/r	27
Auftragsverarbeitung	27
Was tun im Betriebsratsgremium?	28
Strategie des Betriebsrates: vorbereitende Überlegungen	28
Verhandlungsvorbereitung: Fragen an die Geschäftsführung	29
Die Einführung eines HinweisgeberInnen-Systems	30
Muster-Betriebsvereinbarung	32
Anhang	38
Checkliste Betriebsvereinbarung	38
Checkliste für BetriebsrätInnen in der Zusammenarbeit mit hinweisgebenden KollegInnen	38
Checkliste für hinweisgebende ArbeitnehmerInnen	39
Öffentliche Meldestellen in Österreich	40
Stichwortverzeichnis	41

 Zitate

 Wichtige Hinweise

WHISTLEBLOWING

WHISTLEBLOWING – WORUM GEHT'S?

Wer die Trillerpfeife bläst (engl. Whistleblowing), sorgt für Aufmerksamkeit oder schlägt Alarm. Whistleblowing macht sichtbar und hörbar, was oftmals eher unangenehm ist.

Ziel von Whistleblowing ist es, Rechtsverletzungen oder andere gravierende Missstände in Betrieben und Organisationen aufzudecken. Hinweisgebende wollen, dass Missstände behandelt und aufgeklärt werden – anstatt „unter den Teppich gekehrt“. Es geht darum, durch Informationsweitergabe an innerbetriebliche oder außerbetriebliche Stellen eine Veränderung in Gang zu setzen, Untersuchungen zu veranlassen und Abhilfe zu schaffen.

Das Bekanntwerden der Missstände liegt in der Regel auch im Interesse der Öffentlichkeit oder zumindest des Unternehmens (z. B. Verletzung des Umweltschutzes, Gefahr für die Gesundheit, Verletzung des ArbeitnehmerInnenschutzes, Wirtschaftskriminalität, etc.).

Whistleblowing soll also dazu dienen, Missstände aufzudecken und dadurch ein gemeinsames, öffentliches Interesse zu schützen (z. B. den gesunden Arbeitsplatz, die intakte Umwelt).

WhistleblowerInnen haben aufgrund ihrer beruflichen Stellung oft besonderes (Insider-)Wissen über die Vorgänge im Unternehmen. Sie gehen persönliche Risiken ein, da ArbeitgeberInnen und öffentliche Institutionen es in der Regel nicht besonders schätzen, auf

Missstände hingewiesen zu werden. Im Gegenzug für das eingegangene Risiko wird den InformantInnen nun rechtlicher Schutz vor Benachteiligung zugesichert (z. B. durch ein anonymes Meldeverfahren oder die Vertraulichkeit bei der Bearbeitung der Meldung und das Verbot von Repressalien).

AdressatInnen der Informationen über Missstände können direkte oder übergeordnete Vorgesetzte, Aufsichtsgremien, Stabstellen mit besonderen Befugnissen (z. B. Compliance Officer), der Aufsichtsrat, Institutionen außerhalb des Unternehmens, Behörden sowie die gesamte Öffentlichkeit sein.

Abzugrenzen ist Whistleblowing von Intrigen, Wichtigtuerei, Klatsch, Mobbing, übler Nachrede und Verleumdung oder Ähnlichem. In diesen Fällen werden nämlich ausschließlich Eigeninteressen verfolgt und es geht weder um rechtswidriges oder zu missbilligendes Verhalten, noch um eine Warnung oder wesentliche Information für die Öffentlichkeit.

Whistleblowing-Möglichkeiten werden unter Bezeichnungen wie „Compliance-Hotline“, „Meldestelle für Missstände“, „HinweisgeberInnen-System“, oder dergleichen eingerichtet. Es werden AnsprechpartnerInnen genannt, an die man sich bei vermuteten Missständen wenden soll. Es werden (elektronische) Postkästen eingerichtet und/oder Formulare vorgegeben, in denen Beschäftigte Hinweise deponieren sollen. Im Idealfall wird den Hinweisen nachgegangen und der Missstand beseitigt. Dafür braucht es ein verlässliches

right for what is the
relation or from an
point of view.

Whistleblower

who exposes any
of information or
deemed illegal w
right for what is

Prozedere und einen **Schutz der Meldenden und derjenigen, über die gemeldet wird**. Auch BetriebsrätInnen müssen sich daher mit der Gestaltung und Auswirkung von HinweisgeberInnen-Systemen beschäftigen.

WHISTLEBLOWING – WOHER KOMMT'S?

Der Finanzskandal rund um das US-amerikanische Unternehmen Enron hat den Stein ins Rollen gebracht. Der Stromerzeuger mit seiner abenteuerlichen Finanzgebarung löste eine Kettenreaktion aus und legte schlussendlich die Stromversorgung lahm. Im Nachhinein stellte sich heraus, dass auf die Gefahr des Blackouts aufmerksam gemacht wurde. Statt die Missstände zu beseitigen, erhielten die HinweisgeberInnen prompt die Kündigung. Um derartigen Skandalen in Zukunft

vorzubeugen, wurde in den USA ein Gesetz zum Schutz von Hinweisgebenden erlassen, das dazu dienen sollte, WhistleblowerInnen zu ermuntern und nicht abzuschrecken. Das Gesetz dient zwar vor allem dem Schutz von AnlegerInnen, der arbeitsrechtliche Schutz von hinweisgebenden ArbeitnehmerInnen ist darin eher ein Nebenschauplatz, dennoch war es Auslöser für weitreichende Änderungen im europäischen Unternehmens- und Finanzaufsichtsrecht.

Was war passiert? Enron, ein kalifornisch-texanischer Energielieferant mit 22.000 Beschäftigten, hatte sich um das Jahr 2000 in unzählige Finanzgeschäfte verstrickt. Das Register der Verfehlungen beinhaltet falsche Verbuchung von Termingeschäften, illegale Geschäfte mit Offshore-Unternehmen, Bereicherung durch Geschäftsführer, Bilanzfälschung, Abwälzung der Verschuldung

auf anonyme Tochterfirmen, etc. Zusätzlich wurde die Infrastruktur sträflich vernachlässigt und Stromleitungen blieben großflächig unsaniert. Schließlich wurde Enron zahlungsunfähig, die GläubigerInnen hatten das Nachsehen und – der wohl schlimmste Effekt: der gesamte Bundestaat Kalifornien war tagelang von der Stromversorgung abgeschnitten. Die prekären finanziellen Umstände waren einigen der Enron-Beschäftigten bekannt, wurden auch angeprangert, hatten aber außer Entlassungen keine Auswirkung.

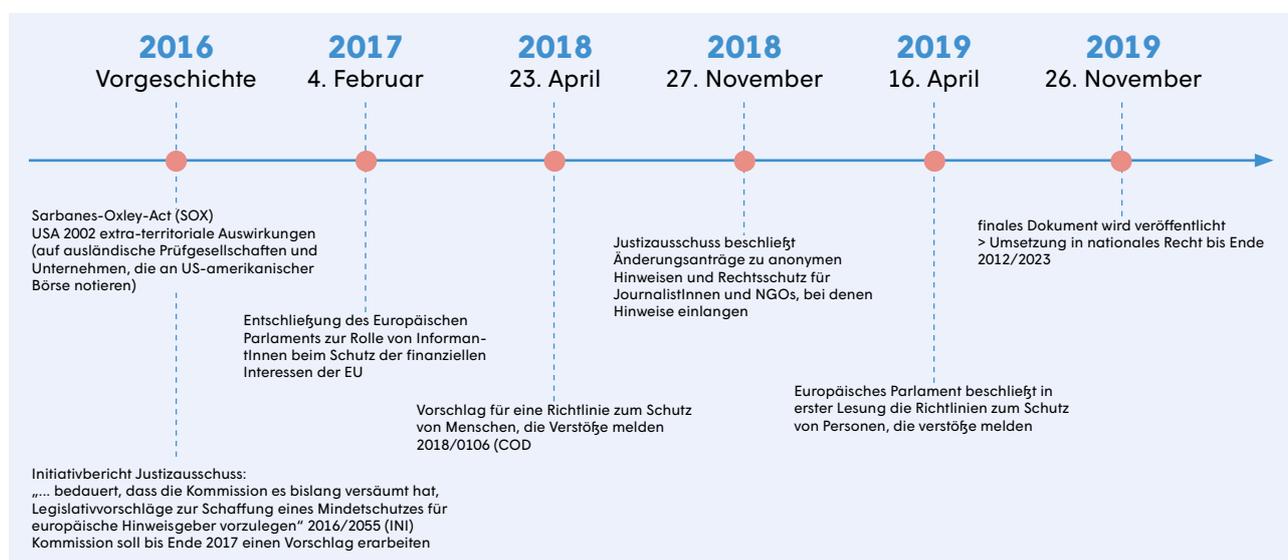
Um einer Wiederholung dieses Desasters zuvorzukommen, wurde 2002 der **Sarbanes-Oxley-Act** (kurz: SOX) verabschiedet. Darin wird Whistleblowing, also das Anprangern von Missständen, für bestimmte Fälle geregelt und MitarbeiterInnen sind seitdem zur Meldung von Verdacht auf wirtschaftliche Schädigung eines börsennotierten Unternehmens verpflichtet. Der Sarbanes-Oxley-Act gilt für Unternehmen, die an der US-amerikanischen Börse notiert sind sowie für deren Töchter, dient also vorrangig dem Anlegerschutz.

Wie kam das Whistleblowing nach Europa? Unternehmen, die an der US-amerikanischen Börse notieren, haben bisweilen auch in Europa Niederlassungen. SOX gilt für den gesamten Konzern unabhängig vom Standort, und somit bestand die Verpflichtung, Whistleblowing-Hotlines auch im europäischen Raum einzurichten, falls Aktien des Mutterunternehmens an der US-amerikanischen Börse gehandelt werden. Auch in Österreich war in internationalen Konzernen seit den 2000er Jahren ein Trend zu Whistleblowing-Hotlines spürbar. Man konnte in der gewerkschaftlichen Beratung beobachten, dass Konzern- und damit

weltweite Hotlines eingerichtet wurden, um rasch von Regelverstößen zu erfahren. Ein Ziel war es dabei sicher auch, Missstände intern „planieren“ zu können und größere finanzielle Verluste sowie Imageschäden in der Öffentlichkeit zu vermeiden. Um das zu erreichen, wurden MitarbeiterInnen dazu angehalten, wenig relevante Verstöße „gegen die Compliance“ zu melden – manchmal unter Missachtung des Datenschutzes und der Mitwirkungsrechte des Betriebsrates.

Vereinzelt gab es in **Europa** einen gesetzlichen Schutz für WhistleblowerInnen, doch der war nur sehr rudimentär vorhanden. Der Schutz, den HinweisgeberInnen in Europa erhielten, war auf nationaler Ebene uneinheitlich gestaltet. Insgesamt hatten bis 2018 zehn EU-Länder (darunter Frankreich, Schweden, Island oder die Slowakei) einen WhistleblowerInnen-Schutz entwickelt. Doch waren Schutzmaßnahmen für die HinweisgeberInnen oftmals nur in einzelnen Branchen (z. B. Finanzsektor, Journalismus) oder nur für bestimmte Missstände (z. B. Korruption) vorhanden.

Mit **berühmten WhistleblowerInnen** in den 2010er-Jahren (z. B. Edward Snowden, Julian Assange, Chelsea Manning) wurde die Diskussion um den Schutz von WhistleblowerInnen auch in Europa lauter. In Deutschland gab es mehrmals öffentliche und parlamentarische Debatten über den gesetzlichen Schutz von HinweisgeberInnen. Die Altenpflegerin Brigitte Heimisch und der Steuerfahnder Rudolf Schmenger erlangten in Deutschland einige Berühmtheit, weil sie innerbetriebliche Missstände aufzeigten und daraufhin entlassen wurden.



HinweisgeberInnen-Systeme erfreuten sich in Europa – zumindest im Jahr 2017 als das Spezial-Eurobarometer zu Korruption durchgeführt wurde – keiner allzu großen Bekanntheit (siehe Grafik).

Die „Europäische Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (2018/0106 (COD))“ sollte das ändern, da sie einen EU-weit einheitlichen Schutz für WhistleblowerInnen bietet. Die Whistleblowing-Richtlinie (WB-RL) ist seit November 2019 in Kraft und muss bis 17. Dezember 2021 bzw. 2023 verbindlich in nationales Recht umgesetzt werden.

Im Europäischen Parlament wurde die Richtlinie zum Schutz von WhistleblowerInnen im April 2019 diskutiert und abgestimmt:



„Der vereinbarte Text verbietet ausdrücklich Repressalien und führt Schutzmaßnahmen ein, damit ein Hinweisgeber nicht entlassen, degradiert, eingeschüchtert oder in anderer Weise angegriffen wird. Auch geschützt wird, wer Hinweisgeber unterstützt, wie zum Beispiel Mittelsmänner, Kollegen oder Verwandte.“
Pressemitteilung Plenartagung 16.4.2019

Im Entwurf der Kommission zur Whistleblowing-Richtlinie¹ wird erklärt in welchem Zusammenhang der Schutz von ArbeitnehmerInnen zu sehen ist und wie er verbessert werden soll:



„Durch einen verbesserten Hinweisgeberschutz wird das Schutzniveau der Arbeitnehmer insgesamt im Einklang mit den Zielen der Europäischen Säule sozialer Rechte und insbesondere gemäß Grundsatz 5 (faire Arbeitsbedingungen) und Grundsatz 7b (Kündigungsschutz) angehoben.“
Entwurf der EU-Kommission (Seite 5)

Unter finnischer Ratspräsidentschaft wurde die Richtlinie zum Schutz von WhistleblowerInnen schließlich im November 2019 unterzeichnet.



„Die EU legt großen Wert auf ein gut funktionierendes demokratisches System, das auf Rechtsstaatlichkeit beruht. Dazu gehört, dass Hinweisgeber, die den Mut haben, sich zu Wort zu melden, überall in der EU ein hohes Maß an Schutz erhalten. Niemand sollte Gefahr laufen, durch das Aufdecken von illegalem Verhalten sein Ansehen oder seinen Arbeitsplatz zu verlieren.“
Anna-Maja Henriksson, finnische Justizministerin

AWARENESS ABOUT THE PROTECTION OF WHISTLEBLOWERS



49 %
of citizens
did not know where to
report corruption



15 %
of citizens
know about existing rules on
whistleblower protection

Quelle: „Factsheet Whistleblowing“ EU-Kommission 2018; https://ec.europa.eu/info/sites/info/files/placeholder_11.pdf (zuletzt abgerufen 12.03.2020)

¹ Vorschlag für eine Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht

DIE EUROPÄISCHE WHISTLEBLOWING-RICHTLINIE

Mit der Whistleblowing-Richtlinie ist nun umfassend geregelt, dass in bestimmten Unternehmen Meldekanäle installiert werden müssen, wie sie gestaltet werden müssen, welche Inhalte gemeldet werden können und vor allem wie und wovor die **HinweisgeberInnen** auf ihren Arbeitsplätzen geschützt werden müssen.

Eine solche EU-weit gültige Vorgabe und deren weitreichender Geltungsbereich sind in vielen Angelegenheiten eine Verbesserung der derzeitigen eher unsicheren und EU-weit uneinheitlichen Lage für Hinweisgebende.

DIE ENTSTEHUNG DER WHISTLEBLOWING-RICHTLINIE

Die EU-Richtlinie muss bis 2021 bzw. 2023 in nationales Recht umgesetzt werden. Diese Vorgaben dürfen von den Mitgliedsstaaten nur beschränkt abgeändert werden. In Österreich wurde die Richtlinie im HinweisgeberInnenschutzgesetz umgesetzt.

PERSONEN, DIE GESCHÜTZT WERDEN

Die Definition der Personen, die von der neuen EU-Richtlinie geschützt sind, ist sehr weitreichend. Es sind sowohl „normale“ ArbeitnehmerInnen umfasst, als auch explizit ArbeitnehmerInnen in **atypischen Beschäftigungsverhältnissen, wie befristet Beschäftigte, LeiharbeiterInnen** und Teilzeitbeschäftigte.

Der Begriff „ArbeitnehmerIn“ schließt **BeamtenInnen**, öffentliche Bedienstete und andere Personen, die im öffentlichen Sektor arbeiten, ein. **Freiwillige und PraktikantInnen**, nicht geschäftsführende Mitglieder, GesellschafterInnen sind ebenso inkludiert wie ArbeitnehmerInnen mit bereits beendeten Vertragsverhältnissen. Außerdem ist in der Richtlinie geregelt, dass allfällig involvierte Dritte, wie Verwandte, KollegInnen oder GewerkschafterInnen, genauso vor Repressalien geschützt werden müssen.

INHALTE, DIE GEMELDET WERDEN

Die Inhalte, die gemäß EU-Richtlinie gemeldet werden sollen, betreffen zahlreiche Rechtsmaterien, für die die EU zuständig ist. Es besteht ein sehr breiter Anwendungsbereich. Die Liste umfasst:

- öffentliches Auftragswesen,
- Verhütung von Geldwäsche,
- Verbraucherschutz, Umweltschutz,
- Lebensmittelsicherheit,
- Tierschutz,
- öffentliche Gesundheit und
- nicht zuletzt geht es um den Schutz der Privatsphäre und personenbezogener Datensicherheit.

Wenn also ein Chemieunternehmen giftige und gesundheitsgefährdende Abwässer – ob beabsichtigt oder nicht – in den Fluss leiten würde, wäre das ein Fall für Whistleblowing. Wenn einem Bank-Unternehmen

personenbezogene Datensätze (z. B. über die Finanzsituation der KundInnen) abhandeln, wäre das ein Fall für Whistleblowing – und für den/die betriebliche/n Datenschutzbeauftragte/n.



Die GPA rät dringend: Nicht jeder kleine Regelverstoß soll an ein Whistleblowing-System gemeldet werden.

Die Mitgliedstaaten können bei der Umsetzung der WB-RL in nationales Recht über diese Liste hinausgehen und sie mit ihren nationalen Rechtsvorschriften in Einklang bringen.

Es steht HinweisgeberInnen selbstverständlich auch dann zu, Missstände zu melden, wenn diese nichts mit den in der EU-Richtlinie angeführten Themen zu tun haben (z. B. bei Diskriminierung aufgrund des Geschlechts oder der sexuellen Orientierung kann man sich an die Gleichbehandlungsanwaltschaft wenden, obwohl das nicht bei den in der EU-Richtlinie angeführten Meldeinhalten enthalten ist).

VERBOTENE REPRESSALIEN AM ARBEITSPLATZ

Generell geht es in der EU-Richtlinie vor allem um den Schutz vor Repressalien am Arbeitsplatz. Hinweisgebende dürfen nicht aufgrund ihrer Hinweise benachteiligt werden. Dieser Schutz ist sehr umfassend definiert. Explizit verboten sind:

- Suspendierung, Kündigung oder vergleichbare Maßnahmen;
- Herabstufung oder Versagung einer Beförderung;
- Aufgabenverlagerung, Änderung des Arbeitsortes, Gehaltsminderung, Änderung der Arbeitszeit;
- Versagung der Teilnahme an Weiterbildungsmaßnahmen;
- negative Leistungsbeurteilung oder Ausstellung eines schlechten Arbeitszeugnisses;
- Disziplinarmaßnahme, Rüge oder sonstige Sanktion einschließlich finanzieller Sanktionen;
- Nötigung, Einschüchterung, Mobbing oder Ausgrenzung;
- Diskriminierung, benachteiligende oder ungleiche Behandlung;

- Nichtumwandlung eines befristeten Arbeitsvertrags in einen unbefristeten Arbeitsvertrag in Fällen, in denen der/die ArbeitnehmerIn zu Recht erwarten durfte, einen unbefristeten Arbeitsvertrag angeboten zu bekommen;
- Nichtverlängerung oder vorzeitige Beendigung eines befristeten Arbeitsvertrags;
- Schädigung (einschließlich Rufschädigung), insbesondere in den sozialen Medien, oder Herbeiführung finanzieller Verluste (einschließlich Auftrags- oder Einnahmeverluste);
- Erfassung von Hinweisgebenden auf „schwarzen Listen“ auf Basis einer informellen oder formellen sektor- oder branchenspezifischen Vereinbarung mit der Folge, dass Hinweisgebende sektor- oder branchenweit keine Beschäftigung mehr finden;
- vorzeitige Kündigung oder Aufhebung eines Vertrags über Waren oder Dienstleistungen;
- Entzug einer Lizenz oder einer Genehmigung;
- psychiatrische oder ärztliche Überweisungen.

DIE MELDESTELLE

Wohin man sich als HinweisgeberIn wendet, ist immer abhängig von

- der Sachlage,
- den Rahmenbedingungen,
- dem betroffenen Unternehmen und
- den involvierten Personen.

Angenommen, jemand findet die Rechnung über ein teures, viel Benzin verbrauchendes Auto in den Unterlagen eines Pharmareferenten/einer Pharmareferentin: das ist vermutlich betriebsintern dann interessant, wenn die Rechnungsadresse von einer Konkurrenzfirmastammt. Man könnte annehmen, dass der Kollege/die Kollegin bestochen wurde – oder es zumindest versucht wurde. Für die breite Öffentlichkeit bestünde eher weniger Interesse an dieser Information und Medien wären eine wenig passende Meldestelle.

Ist hingegen davon auszugehen, dass die Öffentlichkeit großes Interesse an einem bestimmten Fehlverhalten hat (und eine betriebsinterne Meldung kaum bis gar keine Auswirkungen haben würde), wird man sich als HinweisgeberIn eher an eine außerbetriebliche Meldestelle wenden. Beispielsweise wäre selbiger PKW in der Spesenabrechnung des Pressesprechers einer

Umweltschutz-NGO, die sich in einer großen Kampagne gegen Verbrennungsmotoren stark macht, rechtlich zwar vermutlich irrelevant, wohl aber für die Öffentlichkeit relevant.

PFLICHT, EINE MELDESTELLE EINZURICHTEN

Unternehmen haben jedoch nicht die freie Wahl, ob sie eine Meldestelle installieren oder nicht. Meldestellen müssen folgende Unternehmen einrichten (gemäß der EU-Richtlinie, Artikel 4):

- Öffentlicher Sektor (Regierung, Behörden, Gemeinden mit einer Bevölkerung von 10.000 oder mehr)
- private Unternehmen mit 50 oder mehr Beschäftigten (für kleinere Unternehmen kann der nationale Gesetzgeber eigene Regelungen erlassen)
- Sämtliche Unternehmen des Finanzbereichs

Ein Großteil der Beschäftigten in österreichischen Unternehmen – egal ob öffentlich oder privat – wird daher wohl jedenfalls ein Meldesystem zur Verfügung gestellt bekommen und bei einer Meldung weitgehend vor Repressalien geschützt sein.

Unternehmen zwischen 50 und 250 Beschäftigten haben mit der Einrichtung von Meldekanälen bis Ende 2023 Zeit, die öffentliche Verwaltung und Unternehmen mit mehr als 250 Beschäftigten sind bis Ende 2021 verpflichtet, Meldekanäle einzurichten.

EXTERNE MELDESTELLE

Es gibt mehrere Möglichkeiten, wo genau eine Meldestelle eingerichtet wird. Es kann eine externe Stelle ernannt werden (z. B. NGO, Rechtsanwaltskanzlei), aber auch eigens darauf spezialisierte Dienstleister können als Meldestelle eingerichtet werden. Die Europäische Richtlinie zum Schutz von Hinweisgebenden besagt, dass eine Meldestelle für interne Missstände, Fehlentwicklungen und allfällig kriminelles Verhalten auch gemeinsam mit anderen Unternehmen eingerichtet werden kann.

Es kann auch eine **Behörde** zur Ansprechstelle bestimmt werden.

Außerdem können ArbeitnehmerInnen und BetriebsrätInnen **Gewerkschaften, zuständige NGOs oder Medien** verständigen. Die GPA empfiehlt die Meldung an eine externe Stelle allerdings erst dann, wenn

die aufgezeigten Missstände im Betrieb ignoriert werden. Gewerkschaften sind in der Richtlinie explizit als mögliche Meldestellen für betriebliche Missstände genannt (Erwägungsgrund 45).

Die mit der Bearbeitung von Meldungen betraute Stelle muss jedenfalls von den anderen Unternehmenseinheiten in Bezug auf ihre Funktion als Meldestelle strikt getrennt sein. Das heißt, wenn Meldungen vom Unternehmensjuristen entgegengenommen werden, darf dieser nicht mit anderen Abteilungen über die gemeldeten Verdachtsmomente sprechen. In der Meldestelle dürfen ausschließlich Personen arbeiten, die besonders geschult sind und für die Vertraulichkeit der gemeldeten Daten sorgen können.

Abgesehen von den in der EU-Richtlinie genannten Meldestellen und NGOs, können Missstände auch vor den zuständigen Behörden zur Anzeige gebracht werden.

GESTALTUNG DER MELDESTELLE

Wörtlich ist in der Richtlinie festgehalten, dass die Meldekanäle und die Folgemaßnahmen „nach Rücksprache und im Einvernehmen mit den Sozialpartnern“ erfolgen müssen (Art 8).

Hinweisgebende müssen die Möglichkeit haben, ihre Meldungen **anonym** abzugeben. Auf ihren eigenen Wunsch hin können sie ihre Identität gegenüber der Meldestelle offenlegen, was für allfälliges Rückfragen oder Rückmeldungen zu weiteren Nachforschungen wesentlich ist.

Meldekanäle müssen für HinweisgeberInnen **leicht zugänglich** sein. Im Erwägungsgrund 53 der Richtlinie wird ausgeführt, wie ein Meldesystem gestaltet sein soll: „Konkret sollten sie [die Meldekanäle; Anm.] schriftliche Meldungen auf dem **Postweg**, über einen **Beschwerde-Briefkasten** oder über eine **Online-Plattform** (Intranet oder Internet) und/oder mündliche Meldungen über eine **Telefon-Hotline** oder ein anderes System für gesprochene Nachrichten ermöglichen. Im Rahmen dieser Kanäle sollten innerhalb eines angemessenen Zeitraums auf Anfrage des Hinweisgebers auch **physische Zusammenkünfte** stattfinden können.“

Eine Meldestelle, wie der Europäische Gesetzgeber sie vorsieht, muss **auf bestimmte Sachverhalte beschränkt** sein, die **Hinweisgebenden gut schützen** und

muss auch anonyme Meldemöglichkeiten enthalten. Um diese Anforderungen konkret in die betriebliche Praxis umzusetzen, ist der Betriebsrat gefragt und zur Mitsprache verpflichtet. Um die Vorgaben aus der EU-Richtlinie zum Schutz von HinweisgeberInnen im Unternehmen umzusetzen, hält die GPA folgende Punkte in einer BV für wichtig:

- Eine Meldestelle kann in folgender Form eingerichtet werden:
 - Telefon
 - Online-Plattform
 - E-Mail-Postfach
 - Postadresse
 - Briefkasten
 - Ergänzend: face-to-face-Treffen, wenn gewünscht
- **Anonymität und Vertraulichkeit für Hinweisgebende und Beschuldigte** muss gegeben sein. HinweisgeberInnen müssen sich sicher sein können, dass ihre Identität nicht innerhalb des Unternehmens publik gemacht wird, sondern ihr Name – wenn überhaupt – ausschließlich bei der zuständigen Stelle bekannt ist. Sowohl HinweisgeberInnen müssen vor Bloßstellung als auch Beschuldigte vor Verleumdung geschützt sein. Auch Beschuldigte dürfen nicht öffentlich genannt werden, solange Ermittlungen laufen und ausschließlich Verdachtsmomente im Raum stehen.
- Der **Zugang** zu einem elektronischen System sollte auch außerhalb des Betriebes über betriebsfremde Endgeräte und abseits betrieblicher Arbeitszeiten möglich sein. Der Zugang zu einem Postkasten müsste dementsprechend so gestaltet sein, dass eine anonyme Abgabe von Hinweisen möglich ist (z. B. wird der Kasten an einem eher abseits gelegenen Ort installiert, der aber einfach erreichbar ist; es liegen neben dem Kasten großformatige, blickdichte Kuverts bereit).
- Es sollte ein **ausgewogenes und transparentes Verfahren** geben, mit dem Hinweisen behandelt werden. Insbesondere muss die beschuldigte Person die Möglichkeit haben, Stellung zu nehmen bzw. sich entsprechend einzubringen (z. B. indem Einsicht in die eingebrachten Dokumente gewährt wird). Den Beschuldigten ist grundsätzlich Zugang zu den Anschuldigungen einzuräumen. Die beschuldigte(n) Person(en) soll unverzüglich über die Vorwürfe informiert werden – außer es besteht die Gefahr, dass durch die Beteiligung des/der Verdächtigten die

Aufklärung vereitelt wird oder die Gefahr, dass Beweismittel unterschlagen werden könnten.

- Die Verantwortlichkeiten klarzustellen, ist ein wesentliches Element und hilft den HinweisgeberInnen, sich zu orientieren.
 - Wer nimmt Meldungen entgegen?
 - Werden Hinweise an Stellen außerhalb des Betriebs weitergeleitet?
 - Wer gibt den Hinweisgebenden Rückmeldung binnen der vorgegebenen Fristen?
 - Wer hat bei allfälligen Einsichtnahmen das Recht, dabei zu sein?
- Beim betriebsinternen Whistleblowing geben ArbeitnehmerInnen ihre Hinweise i.d.R. an eine eigens dafür vorgesehene Organisationseinheit weiter (z. B. Rechtsabteilung, Revision, „Compliance Officer“). Verantwortlicher im Sinne des Datenschutzrechtes ist immer der/die ArbeitgeberIn.
- Expliziter Ausschluss eines erweiterten Datengebrauchs: Die gemeldeten Missstände sollten nur daraufhin geprüft werden, ob der gemeldete Sachverhalt tatsächlich vorliegt oder nicht. Eine weitere Verwendung der Daten sollte ausdrücklich ausgeschlossen werden (z. B. „Daten-Beifang“ zum Zweck der Leistungskontrolle).
- Information und Schulung für alle MitarbeiterInnen, insbesondere bei der Einführung eines neuen Systems und bei der Einschulung neuer KollegInnen.
- Informations-, Kontroll- und Eingriffsrechte des Betriebsrates festlegen, sofern dies vom Betriebsrat gewünscht wird. Siehe Kapitel „Der Betriebsrat und das Whistleblowing“ (Seite 18 ff).

FRISTEN

Damit WhistleblowerInnen nicht ewig auf eine allfällig gewünschte Rückmeldung warten müssen, sieht die EU-Richtlinie Fristen vor, binnen derer Hinweisgebenden Informationen bzw. Bestätigungen zugesandt werden müssen. So ist festgelegt, dass **unverzüglich spätestens jedoch binnen sieben Tagen** der Eingang einer Meldung bestätigt werden muss.

Über die weiteren Untersuchungsschritte und Folgemaßnahmen müssen Meldende innerhalb von **drei Monaten** Bescheid erhalten.

In der Praxis geht es daher darum, sich die Bestätigung aufzuheben, dass man einen Missstand gemeldet hat bzw. zu beweisen, dass man deshalb einer Benachteiligung ausgesetzt ist.

DIE ÖSTERREICHISCHE UMSETZUNG DER EU-WHISTBLEBLOWING- RICHTLINIE

DAS HINWEISGEBERINNENSCHUTZGESETZ

Grundsätzlich hätte die Umsetzung der EU-Whistleblowing-Richtlinie in das nationale Recht bereits bis 17.12.2021 erfolgen müssen. Die Bundesregierung hat sich jedoch sehr lange Zeit gelassen und erst im Juni 2022 einen Begutachtungsentwurf vorgelegt.

Dieser liegt nun mit einigen kleineren Änderungen als Initiativantrag vor und steht kurz vor Beschlussfassung. Das österreichische Umsetzungsgesetz der Richtlinieninhalte trägt den Titel „**HinweisgeberInnenschutzgesetz**“ (HSchG). Es bildet somit die Rechtsgrundlage für den Schutz von WhistleblowerInnen in Österreich.

Dieses orientiert sich inhaltlich sehr stark an der Richtlinie und geht kaum darüber hinaus. Lediglich um einige Korruptionsdelikte, die im österreichischen Strafgesetzbuch (§§ 30–309 StGB) enthalten sind, wurde der Anwendungsbereich des HSchG über jenen der Richtlinie hinaus erweitert. Dieser Umstand ist besonders schade, weil damit der überwiegende Teil jener – auch strafrechtlich relevanten –

Verfehlungen, zu denen häufig Hinweise gegeben werden, nicht erfasst sind. Insbesondere betrifft dies Delikte wie Untreue und Bilanzfälschung. Auch das gesamte Verwaltungsstrafrecht ist nicht vom HSchG erfasst – beobachten MitarbeiterInnen also Verstöße gegen das Verwaltungsstrafrecht wie Lohndumping, Schwarzarbeit oder Verstöße gegen Vorschriften im Bereich ArbeitnehmerInnenschutz und erstatten sie darüber Meldung, erhalten sie keinen Schutz als WhistleblowerInnen durch das HSchG.

Diese **Unterscheidung in erfasste und nicht erfasste Sachverhalte** wirft bereits ganz grundsätzlich Probleme auf: HinweisgeberInnen, deren Meldungen „thematisch“ in den Anwendungsbereich des Gesetzes fallen, werden geschützt – HinweisgeberInnen, die zwar Verfehlungen beobachten und diese melden, der Gegenstand der Meldung jedoch nicht in den Anwendungsbereich des Gesetzes fällt, sind nicht oder nur in sehr geringem Ausmaß geschützt. Diese Unterscheidung könnte daher auch vor dem Hintergrund des verfassungsrechtlichen Gleichheitsgrundsatzes problematisch sein. Eine deutliche Ausweitung des



Anwendungsbereiches hätte in diesem Zusammenhang also Sinn gemacht.

Im HSchG werden grundsätzlich Unternehmen oder öffentliche Einrichtungen mit mehr als 50 Beschäftigten erfasst. ArbeitnehmerInnen in Unternehmen oder öffentlichen Einrichtungen mit weniger als 50 Beschäftigten kommt daher nach dem Gesetz kein vollumfänglicher Schutz zu. Zwar gibt auch die Richtlinie einen Grenzwert von 50 ArbeitnehmerInnen vor, dieser bezieht sich jedoch nur auf die Pflicht zur Einrichtung interner Meldestellen, nicht jedoch auf den Anwendungsbereich an sich.

Die bereits im Richtlinientext vorgesehene **Beweislastumkehr** wurde durch das HSchG nun auf nationaler Ebene in einem solchen Sinne umgesetzt, dass grundsätzlich das Unternehmen nachweisen muss, dass eine erfolgte Kündigung oder Entlassung durch das Unternehmen gerechtfertigt werden muss, soweit sie im Zusammenhang mit einer Hinweisgebung durch den betroffenen Mitarbeiter oder die betroffene Mitarbeiterin erfolgt ist. Fraglich ist jedoch, ob die österreichische Umsetzung – im Sinne einer Beweiserleichterung – tatsächlich den europarechtlichen Vorgaben durch die

Richtlinie entspricht und nicht wesentlich stärker hätte ausgestaltet werden müssen.

Das österreichische HSchG legt für bestimmte Fälle auch Verwaltungsstrafen fest bzw. konkretisiert die in der EU-Richtlinie normierte **Pflicht zur Festlegung von Sanktionen**. Vorgesehen sind Geldstrafen bis zu maximal 20.000 Euro bzw. bis zu maximal 40.000 Euro im Wiederholungsfall. Diese drohen immer dann, wenn Unternehmen versuchen, HinweisgeberInnen bei der Erstattung einer Meldung zu behindern oder auf andere Weise unter Druck setzen, etwa indem gerichtliche oder behördliche Verfahren angestrengt werden. Strafen drohen auch dann, wenn ArbeitgeberInnen – auf welche Weise auch immer – Rache oder „Vergeltung“ an den HinweisgeberInnen üben oder die gesetzlich zugesicherte Vertraulichkeit der Meldung verletzen.

Kritikwürdig an dieser Art der Umsetzung erscheint insbesondere der sehr niedrig angesetzte Strafrahmen. Während in der Richtlinie betont wird, die in Aussicht gestellten Sanktionen müssten wirksam, angemessen und abschreckend sein, ist dies bei einer Strafdrohung von höchstens 20.000 Euro bzw. 40.000 Euro (im Wiederholungsfall) wohl kaum gewährleistet.

DER BETRIEBSRAT UND DAS WHISTLEBLOWING

Die tägliche Betriebsratsarbeit stützt sich auf das Arbeitsverfassungsgesetz (ArbVG). Im ArbVG sind die Grundlagen für die betriebliche Interessenvertretung allgemein festgelegt. Es ist geregelt, wofür der Betriebsrat zuständig ist, welche Instrumente für die Interessenvertretung der Belegschaft genutzt werden können, wer zur betriebsrätlichen Arbeit hinzugezogen werden kann, wie die Mitglieder des Betriebsrates gewählt und geschützt werden, etc. Auch die EU Kommission betont in ihrem Vorschlag zur Whistleblowing-Richtlinie (S. 6)², dass Arbeitsrecht, ArbeitnehmerInnenschutz und HinweisgeberInnenschutz nebeneinander bestehen sollen



„Hinweisgeberschutz in einem Arbeitskontext besteht zusätzlich zu dem Schutz, den Arbeitnehmer und Arbeitnehmer-Vertreter im Rahmen des bestehenden EU-Arbeitsrechts genießen, wenn sie gegenüber Ihren Arbeitgebern Probleme mit der Einhaltung von Vorschriften ansprechen. Dies betrifft insbesondere die Einhaltung von Vorschriften im Bereich der Sicherheit und Gesundheit am Arbeitsplatz (...). Die Kommission möchte (...) auch die Durchsetzung und Einhaltung des geltenden EU-Rechtsrahmens im Arbeitnehmerschutz verbessern.“

Arbeitsrechtlich betrachtet handelt es sich bei Whistleblowing-Systemen im Betrieb in der Regel um **Kontrollsysteme, die die Menschenwürde berühren**. Daher sind die Mitwirkungsrechte des Betriebsrates (insbes. § 96 ArbVG, siehe auch Kapitel „Whistleblowing und Arbeitsrecht“ (Seite 22 ff), ebenso zu beachten wie die Rechte der einzelnen ArbeitnehmerInnen (§ 10 AVRAG). Das heißt: die Mitwirkungsrechte, die kollektiv im ArbVG und individuell im AVRAG verankert sind, bleiben ungeschmälert aufrecht und gelten zusätzlich zum Schutz durch die Richtlinie.

ZUSÄTZLICHER SCHUTZ DES BETRIEBSRATSMITGLIEDS

Zusätzlich zum Schutz, den die EU-Richtlinie WhistleblowerInnen bietet, besteht durch das österreichische Arbeitsverfassungsgesetz ein gewisses Maß an Schutz für Mitglieder des Betriebsrats – solange sie im Rahmen ihrer betriebsrätlichen Aufgaben handeln. BetriebsrätInnen verfügen über besondere gesetzliche Instrumente, damit sie ihrer Tätigkeit im Rahmen der Interessenvertretung nachkommen können und nicht behindert werden.

² Vorschlag für eine Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. EU-Kommission, Brüssel 2018/0106 (COD). In den Erwägungsgründen 21 und 29 der beschlossenen Richtlinie finden sich diese Überlegungen wieder.



Für BetriebsrätInnen, die in Ausübung ihrer betriebsrätlichen Funktion Missstände aufdecken, Beschäftigte beraten oder selbst als Anlaufstelle tätig sind, gelten also neben dem Schutz aus der EU-Richtlinie weitere besondere Rechte aus dem ArbVG. Diese arbeitsrechtlichen Regeln werden explizit nicht von der Richtlinie berührt, gelten also weiter.³

Ein Betriebsratsmitglied ist durch einen besonderen **Kündigungs- und Entlassungsschutz** abgesichert (§ 120 Abs 1 ArbVG). Der/die ArbeitgeberIn darf ein Mitglied des Betriebsrates ausschließlich dann kündigen oder entlassen, wenn ein Gericht zugestimmt hat. Beendet der/die ArbeitgeberIn das Arbeitsverhältnis mit einem Betriebsratsmitglied ohne gerichtliche Zustimmung, so ist diese Handlung nichtig – das Arbeitsverhältnis bleibt also weiterhin unverändert aufrecht. Sollte ein Betriebsrat/eine Betriebsrätin aufgrund der Meldung eines Missstandes gekündigt oder entlassen werden, kann er/sie sich vor Gericht grundsätzlich darauf berufen, dass er/sie diese Meldung aufgrund seiner betriebsrätlichen Arbeit erstattet hat und die Entlassung somit rechtsunwirksam ist.

Die betriebsrätlichen Mitwirkungsrechte umfassen zunächst ein **Interventionsrecht** (§ 90 Abs 1 ArbVG). Das bedeutet, der Betriebsrat hat das Recht, Maßnahmen vorzuschlagen und zu beantragen, um die Arbeitsbedingungen zu verbessern, Mängel zu beheben, Korrekturen vorzunehmen, etc. Dazu gehört, dass Maßnahmen zur Einhaltung von Rechtsvorschriften beantragt werden können und Verfehlungen und Rechtsverstöße im Unternehmen thematisiert werden. Kurz gesagt, er/sie darf Missstände, die die Beschäftigten betreffen, aufzeigen und anprangern.

Interventionen müssen jedoch nicht zwingend intern bleiben, sondern können auch **außerbetrieblich** erfolgen. Bei einer Intervention an eine Stelle außerhalb des Betriebs ist vorab abzuwägen, ob die Interessen der Belegschaft oder jene des/der BetriebsinhaberIn überwiegen, weshalb eine Intervention in der Regel zunächst intern vorgenommen werden wird.

Ist eine erste Intervention beim/bei der ArbeitgeberIn erfolglos, können sich BetriebsrätInnen selbstverständlich an **Behörden** wenden um einen aus ihrer Sicht strafbaren Sachverhalt anzuzeigen. BetriebsrätInnen könnten sich im Zusammenhang mit Whistleblowing auch an **externe Meldestellen** wenden (siehe Anhang).

Damit BetriebsrätInnen ungehindert arbeiten und die Interessen der Belegschaft wirksam vertreten können, besteht dem Gesetz zufolge ein sogenannter **Beschränkungs-, Benachteiligungs- und Versetzungsschutz** (gem. § 115 Abs 3 ArbVG). Dieser Schutz bezieht sich auf das Entgelt, Schulungsteilnahmen oder Aufstiegsmöglichkeiten, die aufgrund der betriebsrätlichen Tätigkeit nicht eingeschränkt werden dürfen.

BetriebsrätInnen werden sich daher in der Regel zur Konsultation an außerbetriebliche Stellen wenden dürfen. Andernfalls würde eine „Behinderung in der Mandatsausübung“ vorliegen. Ebenso darf es den Beschäftigten nicht erschwert werden, **sich an den BR zu wenden**. ArbeitnehmerInnen können sich mit Meldungen über Verfehlungen oder Verstöße grundsätzlich an den Betriebsrat wenden und müssen nicht zwingend das vom Unternehmen eingerichtete Whistleblowing-System nutzen.

Weisungen können Betriebsratsmitgliedern bei der Ausübung ihrer Tätigkeit ohnehin nicht erteilt werden (gemäß § 115 Abs 2 ArbVG). Eine Weisung des Vorgesetzten, etwas nicht oder schon zu melden, hätte keine rechtliche Wirkung.

Dem Betriebsrat steht das Recht zu, sobald die Interessen der ArbeitnehmerInnen berührt sind, die **Gewerkschaft oder Arbeiterkammer zu Beratungen hinzuziehen** (gemäß § 92 Abs 2 ArbVG), so auch in Fragen, die sich in Zusammenhang mit dem Whistleblowing ergeben.

Bei ArbeitnehmerInnen, die keine Betriebsratsmitglieder sind, besteht kein derart ausgeprägter Schutz. Nachdem ArbeitnehmerInnen in Österreich grundsätzlich ohne Angabe von Gründen jederzeit (unter Einhaltung der Fristen) gekündigt werden können, gilt das – problematischerweise – auch für Ersatzmitglieder im Betriebsrat. Deshalb hat die Umsetzung der EU-Whistleblowing-

³ Siehe Erwägungsgründe 21 und 29 der EU Richtlinie zum Schutz von WhistleblowerInnen.

Richtlinie für sie umso entscheidendere Bedeutung, da so ein Mindestmaß an Schutz für alle Missstände meldende ArbeitnehmerInnen hergestellt wird.

GESETZLICHE GRUNDLAGEN FÜR DIE BETRIEBSVEREINBARUNG (BV)

Die Einführung von Whistleblowing-Systemen erfordert in der Regel die Zustimmung des Betriebsrates mittels einer Betriebsvereinbarung, was sich aus dem ArbVG ergibt.

Es handelt sich bei Whistleblowing-Systemen meistens um **Kontrollmaßnahmen, die die Menschenwürde berühren** (§ 96 Abs 1 Z 3 ArbVG). Unter Kontrollmaßnahmen werden alle zur Überwachung von ArbeitnehmerInnen geeigneten menschlichen Verhaltensweisen und technischen Vorrichtungen verstanden. Dabei ist unerheblich, ob es sich um einen altmodischen Briefkasten an der Wand handelt oder ob es sich bei der konkreten Umsetzung eines Whistleblowing-Systems um eine Telefon-Hotline oder eine online-Plattform handelt. Derartige Maßnahmen sind stets mittels einer Betriebsvereinbarung, also unter Mitbestimmung des Betriebsrates, zu regeln. Im Kern geht es dabei um die systematische Überwachung von Eigenschaften, Handlungen oder des allgemeinen Verhaltens von ArbeitnehmerInnen durch den/die ArbeitgeberIn, wobei es keine Rolle spielt, ob ArbeitgeberInnen die Kontrolle selbst durchführen oder eine/n VertreterIn oder eine dritte Person damit beauftragen.

Beruhet das Whistleblowing-System auf **automationsunterstützter Datenerfassung, -verarbeitung bzw. -weitergabe**, so bedarf es ebenfalls – und unabhängig von einer möglichen Zustimmungsnotwendigkeit gem. § 96 Abs 1 Z 3 ArbVG) – der Zustimmung des Betriebsrates (gem. § 96a Abs 1 Z 1 ArbVG). Diese kann jedoch durch die Entscheidung der Schlichtungsstelle ersetzt werden.

Wird das Whistleblowing-System im Rahmen einer betrieblichen Ordnungsvorschrift genutzt oder dem System eine **Ordnungsvorschrift** zugrunde gelegt, so ist eine Betriebsvereinbarung über die Schlichtungsstelle durch den Betriebsrat erzwingbar (gem. **§ 97 Abs 1 Z 1 ArbVG**).



Ein betriebliches HinweisgeberInnen-System muss mit einer Betriebsvereinbarung (BV) geregelt werden. In der BV wird das jeweilige System konkret vereinbart und das Vorgehen bei Whistleblowing näher beschrieben. In der BV steht, wohin HinweisgeberInnen sich wenden können, wie mit Hinweisen umzugehen ist, wer wann wöber in welcher Form informiert wird, etc.

Damit der im Rahmen der EU-Richtlinie zu gewährleistende Schutz für WhistleblowerInnen nicht konterkariert wird, damit das Arbeitsverfassungsgesetz eingehalten und damit eine gute Betriebskultur aufrechterhalten wird, ist also eine Betriebsvereinbarung abzuschließen.



WHISTLEBLOWING UND ARBEITSRECHT

KEINE GENERELLE MELDEPFLICHT

Eine generelle Verpflichtung zur Meldung von Missständen in einem Whistleblowing-System gibt es in Österreich nicht. Whistleblowing-Systeme im Sinne der Europäischen Richtlinie stellen ausschließlich freiwillige Kanäle dar, in denen auf (beobachtete und vermutete) Missstände aufmerksam gemacht werden kann.

Darüber hinaus bestehen in manchen **Branchen eigene Meldeverpflichtungen** aufgrund spezieller gesetzlicher Vorgaben. Es ist daher zwischen **gesetzlichen Meldepflichten** und **Whistleblowing-Systemen im Sinne der Europäischen Richtlinie** immer zu unterscheiden, welcher Missstand in welchem Unternehmen genau vorliegt und wer unter Umständen verpflichtet ist, Meldung zu erstatten. Wird beispielsweise der Verdacht erhoben, eine Kantinen-MitarbeiterIn habe eine Salmonelleninfektion, ist das nicht vorrangig ein Thema, das über ein Whistleblowing-System gemeldet werden sollte. Vielmehr muss in erster Linie die/der behandelnde Ärztin/Arzt die Gesundheitsbehörde kontaktiert werden.

Je nach Aufgabe und Verantwortungsgrad können einzelne Beschäftigte dazu verpflichtet sein, auf Missstände hinzuweisen. Beispielsweise muss der/die **Brandschutzbeauftragte** darauf hinweisen, wenn Fluchtwege verstellt sind oder Brandschutztüren klemmen.

Individuelle Meldepflichten könnten sich, neben der konkreten Tätigkeit des/der Beschäftigten, aus vertraglichen Verpflichtungen und allenfalls aus der Treuepflicht der ArbeitnehmerInnen ableiten lassen. Dies vor allem, wenn dem Unternehmen großer Schaden in jenem Bereich droht, für dessen Überwachung und Absicherung die jeweiligen MitarbeiterInnen explizit zuständig sind. Beispielsweise wird der/die **Umweltbeauftragte** es wohl melden müssen, wenn große Mengen von Schadstoffen in einen Fluss gespült werden, weil etwa Reinigungsfilter nicht einwandfrei funktionieren.



Beschäftigte können nicht generell verpflichtet werden, alles und jedes zu melden. Die GPA rät daher, **keine zusätzlichen Meldepflichten in Betriebsvereinbarungen zu vereinbaren** (z. B. Meldung von individuellen Verhaltensweisen wie Unpünktlichkeit oder Unfreundlichkeit über das Whistleblowing-System). Derartige Verhaltensvorgaben, allgemeine Verweise auf interne Verhaltensrichtlinien (Code of Conduct) **oder** Weisungen sollten nicht entgegengenommen und keinesfalls unterschrieben werden!

DIE TREUEPFLICHT BEGRÜNDET NOCH KEINE VERSCHWIEGENHEITSPFLICHT

Dass WhistleblowerInnen die Treuepflicht verletzen würden, „QuerulantInnen“ oder „NestbeschmutzerInnen“ seien, ist ein gerne vorgeschobenes Argument,

um unangenehme Meldungen zu unterbinden. Konkret ergibt sich aus der Treuepflicht des/der ArbeitnehmerIn noch längst keine Verpflichtung, über sämtliche Vorgänge im Unternehmen Verschwiegenheit zu bewahren. Wer Missstände aufdeckt, vermutet in der Regel einen Rechtsbruch und erstattet eine entsprechende Meldung, gerade weil er/sie für das Unternehmen Schlimmes befürchtet und es davor bewahren möchte. Hinweisgebende nehmen also die Treuepflicht besonders ernst. Jemand, der absichtlich wegsieht und eine Meldung unterlässt, verletzt die Treuepflicht wohl eher.

Zudem ist festzuhalten, dass gesetzwidriges Verhalten des/der ArbeitgeberIn nicht der Treuepflicht unterliegt. Somit sind ArbeitnehmerInnen **im Interesse der Allgemeinheit** grundsätzlich zu einer Meldung oder in bestimmten Fällen sogar Strafanzeige gegen den/die eigene ArbeitgeberIn berechtigt. Bei einer solchen Strafanzeige haben ArbeitnehmerInnen jedoch eine möglichst schonende Form zu wählen.

Vorwürfe dem/der ArbeitgeberIn gegenüber müssen ein Mindestmaß an Substanz beinhalten, weshalb dringend geraten wird, einer Meldung Belege/Beweise/Dokumente etc. beizulegen. Werden haltlose und unbegründete (oder sogar absichtlich falsche) Anschuldigungen erhoben, kann **Vertrauensunwürdigkeit entstehen und dadurch ein Entlassungsgrund** gesetzt werden.

Wie es mit der Treuepflicht und dem Anzeigen von Straftaten im Arbeitsverhältnis bestellt ist, hat der OGH in einem Rechtssatz dargestellt.⁴



„Den Dienstnehmer trifft bei strafrechtswidrigen Umtrieben des Dienstgebers keine Verschwiegenheitspflicht. Unlautere Geschäftspraktiken oder gesetzwidriges Verhalten zählen nicht zu den Umständen, an deren Geheimhaltung der Arbeitgeber ein objektiv berechtigtes Interesse hat. Wenn es um die Aufdeckung strafrechtlich relevanter Umstände geht, ist ein Dienstnehmer im Interesse der Allgemeinheit auch zur Erstattung einer Strafanzeige berechtigt, wobei er allerdings in einer für den Dienstgeber möglichst schonenden Form vorzugehen hat. Nur haltlose und subjektiv unbegründete Anschuldigungen bilden den Entlassungsgrund der Vertrauensunwürdigkeit.“ (siehe RS0113682)

WHISTLEBLOWING UND DAS GESCHÄFTSGEHEIMNIS

Mitunter wird HinweisgeberInnen auch unterstellt, sie würden Geheimnisverrat begehen. Steht der Vorwurf im Raum, sich eines strafrechtlichen Delikts schuldig zu machen, wird es weitaus schwieriger, sich zu einer Meldung durchzuringen. Diese „Keule“ eignet sich bei näherer Betrachtung jedoch nur bedingt, um WhistleblowerInnen zum Schweigen zu bringen.

Zwar handelt es sich bei HinweisgeberInnen oftmals um Personen mit besonderem Insider-Wissen, doch ist

nicht jedes Insider-Wissen als Geschäftsgeheimnis zu werten. Daher ist eine Offenlegung von Insider-Wissen nicht automatisch als Geheimnisverrat strafbar. Und selbst wenn der Inhalt einer Meldung im Sinne der Whistleblowing-Richtlinie ein Geschäftsgeheimnis offenbaren sollte, kann es sein, dass die Meldung rechtmäßig war (z. B. wenn das Geschäftsgeheimnis gegen Unionsrecht bei Umweltauflagen verstößt, weil es auf die Manipulation von Abgasmessungen hinausläuft).

Was tatsächlich unter den Begriff Geschäftsgeheimnis fällt, wurde 2016 in einer EU-Richtlinie klar definiert. Eine wesentliche Eigenschaft von derartigen Geheimnissen ist, dass sie vor unbefugtem Zugriff geschützt werden müssen und nicht jeder und jedem im Betrieb zugänglich sind. Eine Notiz am „schwarzen Brett“, eine Information im Intranet, eine Anweisung wie gearbeitet werden muss oder wie die Arbeitszeiterfassung zu erfolgen hat, sind daher sicher nicht als geheim zu klassifizieren. (Näheres ist in der EU-Richtlinie zu Geschäftsgeheimnissen⁵ geregelt.) Und auch in einem solchen Fall kann Whistleblowing notwendig sein.

Ein vertrauliches Beratungsgespräch mit den gewerkschaftlichen ArbeitsrechtsexpertInnen kann helfen, die Situation und allfällige Risiken abzuwägen und um die Entscheidung, ob und auf welchem Weg ein Hinweis gegeben wird, auf Basis rechtlicher Einschätzungen zu treffen.

WHISTLEBLOWING UND COMPLIANCE/ VERHALTENSRICHTLINIEN

Viele Unternehmen legen Verhaltensrichtlinien fest, die beschreiben, welches Verhalten ein Unternehmen von den Beschäftigten erwartet und welches Verhalten unerwünscht bzw. untersagt ist. Solche Richtlinien tragen unterschiedlichste Bezeichnungen (z. B. (Konzern-) Verhaltenskodex, Ethik-Charta, Code of Conduct, Corporate Social Responsibility Principles oder auch Compliance Policy).⁶ Bisweilen wird diese Verhaltensvorgabe mit einem Whistleblowing-System kombiniert, damit das Unternehmen über Regelverstöße einfacher bzw. schneller Kenntnis erlangt, reagieren und damit (Image-)Schäden abwenden kann.

⁴ siehe Rechtsprechung des OGH; RIS-Justiz RS0113682

⁵ Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

⁶ Die GPA hat zu dem Thema eine eigene Broschüre veröffentlicht: „Verhaltenskodices, von Corporate Social Responsibility (CSR) zur Compliance Management.“; die Mitglieder auf der Homepage herunterladen oder im Servicecenter bestellen können.

An der Schnittstelle zwischen Compliance Policy und Whistleblowing treten häufig Interessensgegensätze zutage. Nun besteht zwar die Verpflichtung eine Meldestelle einzuführen, aber nicht vorwiegend auf der Basis einer unternehmensinternen Richtlinie. Rechtsgrundlage für die Einrichtung einer Meldestelle bildet vielmehr die Europäische Richtlinie zum Whistleblowing.

Eine „Verhaltensrichtlinie“ ist nämlich im Stufenbau der Rechtsordnung – und daher auch in der Verbindlichkeit – weit unterhalb von EU-Richtlinien angesiedelt. Auch nationales Recht (z. B. ArbVG) oder kollektive Vereinbarungen wie beispielsweise eine Betriebsvereinbarung, stehen über einer betrieblichen Verhaltensrichtlinie.



Eine „Verhaltensrichtlinie“ kann niemals gesetzliche, kollektivvertragliche oder in einer Betriebsvereinbarung festgelegte Rechte und Pflichten außer Kraft setzen.

Ein Verhaltenskodex (auch unter den Namen Code of Conduct, Compliance Code, interne Verhaltensrichtlinie, und Ähnlichem bekannt) kann im Zusammenhang mit einem HinweisgeberInnensystem als Vorwand dienen, angebliches Fehlverhalten von KollegInnen melden zu „müssen“. So kann bei den Beschäftigten der Anschein erweckt werden, sie müssten nun alles und jedes melden (z. B. Unpünktlichkeit, Unfreundlichkeit oder andere „Verstöße gegen den Verhaltenskodex“). Auf diese Art könnte der/die ArbeitgeberIn überschießende Verhaltenskontrollen umsetzen. Für das Betriebsklima können derartige Systeme problematische Folgen mit sich bringen, da sie einer „Vernaderungskultur“ Vorschub leisten. Eine gute Betriebsvereinbarung kann das verhindern.

WEITERE RECHTSGRUNDLAGEN FÜR WHISTLEBLOWING-SYSTEME

Was das österreichische Bankwesen und US-amerikanische börsennotierte Konzerne gemeinsam haben? Sie waren die ersten Unternehmen deren Niederlassungen und Filialen zur Einführung von Melde-Hotlines verpflichtet wurden. Zusätzlich zur Europäischen Richtlinie zum Schutz von HinweisgeberInnen existieren also weitere Rechtsgrundlagen auf die sich HinweisgeberInnen stützen können, um zu untermauern, warum sie sich zum Whistleblowing entschlossen haben.

Eine seit 2002 bestehende Rechtsgrundlage für das Einrichten von Melde-Hotlines ist der Sarbanes-Oxley-Act (**SOX**). Dieses Gesetz gilt allerdings nur für europäische Niederlassungen von Konzernen, die an der US-amerikanischen Börse notieren. Siehe auch Kapitel „Whistleblowing“ (Seite 8 f).

Der Schutz von WhistleblowerInnen ist darin nur spärlich vorhanden.

WHISTLEBLOWING UND DATENSCHUTZ

Zusätzlich zu jenen aus der Whistleblowing-Richtlinie müssen weitere Rechtsmaterien berücksichtigt werden. So sind etwa datenschutzrechtliche Aspekte zu beachten, wenn es um Fragen der Gestaltung des HinweisgeberInnen-Systems geht.

INFORMATION FÜR ARBEITNEHMERINNEN

Es besteht die Pflicht, ArbeitnehmerInnen über die Einrichtung einer Meldestelle zu informieren. Ein HinweisgeberInnen-System verarbeitet personenbezogene Daten, deshalb muss den Betroffenen eine Basisinformation zu dieser Datenverwendung gegeben werden. Die Information muss Angaben darüber erhalten,

- wer die Daten verarbeitet,
- an wen sie allenfalls weitergeleitet werden,
- wozu die Daten verwendet werden und
- wie lange sie gespeichert werden.

Auch den Beschuldigten stehen gewisse Informationen zu, wenn über ihre Person Hinweise eingegangen sind. Wenn es allerdings zum Schutz der Identität der HinweisgeberIn oder zur Unterbindung von Versuchen der Verhinderung, Unterlaufung oder Verschleppung von Hinweisen oder deren Folgemaßnahmen notwendig ist, sind folgende Betroffenenrechte nach DSGVO **nicht** anzuwenden:

- Recht auf Information Art. 13 und 14 DSGVO),
- Recht auf Auskunft (Art. 15 DSGVO),
- Recht auf Berichtigung Art. 16 DSGVO),
- Recht auf Löschung Art. 17 DSGVO),

- Recht auf Einschränkung der Verarbeitung Art. 18 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO) sowie
- Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten Art. 34 DSGVO).

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Der Gesetzgeber hat im Gesetzgebungsprozess eine allgemeine Datenschutz-Folgenabschätzung für die Einrichtung eines Whistleblowing-Systems erstellt. Diese findet sich als Anhang im Gesetzestext. Für HinweisgeberInnen-Systeme, die nicht über die gesetzlich festgelegte Datenverarbeitung hinausgehen, kann daher auf die Durchführung einer Datenschutz-Folgenabschätzung verzichtet werden.

Bei HinweisgeberInnen-Systemen, die über den im HSchG gesetzlich festgelegten Rahmen hinausgehen, z. B. durch eine Erweiterung der möglichen zu meldenden Themen, muss mit hoher Wahrscheinlichkeit eine Datenschutz-Folgenabschätzung (DSFA) gemäß Artikel 35 DSGVO bezüglich der Meldestelle durchgeführt werden.

Bei der Durchführung einer Datenschutz-Folgenabschätzung müssen die **Standpunkte der Betroffenen** (also der Beschäftigten) und ihrer **VertreterInnen** (also des Betriebsrates) eingeholt werden. Außerdem muss bei der Folgenabschätzung darauf geachtet werden, dass Abhilfemaßnahmen geschaffen werden, damit die Betroffenen möglichst wenig in ihrer Privatsphäre

beeinträchtigt werden und auch die technische Sicherheit gewährleistet ist (z. B. eine anonyme Meldestelle, eine Erreichbarkeit außerhalb der Normalarbeitszeit, ein guter Zugriffsschutz der gemeldeten Inhalte etc.).

Um festzustellen, ob eine Datenschutz-Folgenabschätzung (DSFA) benötigt wird, ist eine sogenannte „**Schwellenwertanalyse**“ angebracht. Hier wird überprüft, ob die „Rechte und Freiheiten der Betroffenen“ in einem Ausmaß gefährdet sind, dass eine DSFA erforderlich ist. Die Durchführung einer Schwellenwertanalyse empfiehlt sich insbesondere für HinweisgeberInnen-Systeme, welche schon vor Inkrafttreten des HSchG im Betrieb waren und deren Datenverarbeitung ggf. über den gesetzlich festgelegten Rahmen des HSchG hinausgeht.

DAS VERARBEITUNGSVERZEICHNIS

Der Betrieb als datenschutzrechtlich Verantwortlicher muss das HinweisgeberInnen-System in sein Verzeichnis der Verarbeitungstätigkeiten aufnehmen. Es ist u.a. darin zu dokumentieren, welche personenbezogenen Daten, zu welchem Zweck verarbeitet werden und welche Technisch-Organisatorischen Maßnahmen (TOMs) zur Sicherheit der Verarbeitung ergriffen wurden.

DIE/DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE/R

Wurde im Betrieb ein/e Datenschutzbeauftragte/r ernannt, ist er/sie über die wichtigsten Eckpunkte des Systems im Bilde (z. B. welche personenbezogenen Daten werden erfasst, wer sind weitere Empfängerkreise, wann wird gelöscht, wo steht der Server, etc.) und hat raschen Zugang zur Dokumentation. Die Zusammenarbeit zwischen Datenschutzbeauftragter und dem Betriebsrat einen besseren Wissenstand über das HinweisgeberInnen-System zu erhalten.

AUFTRAGSVERARBEITUNG

Wird das betriebliche HinweisgeberInnen-System von einem externen Dienstleister betrieben, ist mit diesem schriftlich eine Auftragsverarbeitungsvereinbarung nach Art 28 DGSVO abzuschließen. Diese Vereinbarung gewährleistet, dass der Dienstleister nur in dokumentierter Weise personenbezogene Daten verarbeitet und ausreichend Maßnahmen getroffen wurden, um die Verschwiegenheit und die Sicherheit der Verarbeitung zu garantieren. Der Betriebsrat kann sich diesen Vertrag zur Kontrolle vorlegen lassen.

WAS TUN IM BETRIEBSRATSGREMIUM?

STRATEGIE DES BETRIEBSRATES: VORBEREITENDE ÜBERLEGUNGEN

Vor Beginn der konkreten Verhandlungen über eine Whistleblowing-Betriebsvereinbarung sollte die Betriebsratskörperschaft einige grundlegende Positionen zu Whistleblowing überlegen. Wie sehen wir im Betriebsrat eigentlich das Thema? Was wollen wir diesbezüglich erreichen oder vermeiden? Eine interne Diskussion kann anhand der folgenden Leitfragen gestartet werden.

Wie stehen wir zu Whistleblowing?

Was erhoffen wir uns davon, was befürchten wir als Betriebsrat? Was bringt es den KollegInnen? Kann Schaden für KollegInnen entstehen? Sind ArbeitnehmerInnen geschützt vor „Vernachlässigung“? Könnten Probleme mit der Einrichtung einer Meldestelle einhergehen? Können wir dadurch Probleme lösen? Welche Folgen könnte das HinweisgeberInnen-System für die Betriebskultur generell haben? Ermöglicht Whistleblowing eine bessere interne Kommunikation?

Ist das geplante System seriös, oder eher eine „Alibihandlung“?

Gibt es dazu allgemein verständliche Informationen? Was ist das deklarierte Ziel der Meldestelle? Wird dadurch ein angstfreies Aufzeigen von Missständen wirklich erleichtert? Hat der Anbieter bereits andere Systeme (in unserer Branche) installiert und können wir auf

die Erfahrungen der anderen Unternehmen aufbauen?

Wie bringt sich der Betriebsrat bei der Einrichtung des HinweisgeberInnen-Systems ein?

Ist es uns als Betriebsrat wichtig, KollegInnen auch über die konkrete Handhabung zu informieren (z. B., dass bestimmte „Fehler“ nicht gemeldet werden müssen)? Wollen wir als Betriebsrat mitverantwortlich für das HinweisgeberInnen-System sein? Wollen wir hier eine eigene Rolle spielen, beispielsweise Einsichts- und Reportingrechte für den Betriebsrat reklamieren oder wollen wir damit eher nicht in Verbindung gebracht werden?

Passt das (geplante) System zur Belegschaft?

Welche Meldemöglichkeiten beinhaltet das System (sowohl inhaltlich als auch nach der Art und Weise wie gemeldet werden kann)? Welche MitarbeiterInnen-Gruppen haben wir im Betrieb? Ein technisches System, das digitale Vorkenntnisse erfordert, wird in einem Betrieb, in dem nur wenige MitarbeiterInnen Zugang zu einem PC haben, nicht geeignet sein. Umgekehrt wird ein Postkasten in einem gänzlich digitalarbeitenden Betrieb vermutlich eher nicht angenommen.

Passen die innerbetrieblichen Voraussetzungen zum (geplanten) System?

Welches Regelwerk gibt es im Unternehmen schon rund um das Thema Whistleblowing (z. B. Code of

Conduct, Verhaltensrichtlinien, betriebliches Beschwerdemanagement, Kontinuierlicher Verbesserungsprozess, 360°-Feedback etc.)? Sind die bestehenden Vorgaben im Einklang mit dem neuen HinweisgeberInnen-System? Gibt es dazu eine Betriebsvereinbarung im Unternehmen (z. B. in puncto ArbeitnehmerInnen-Datenschutz, Evaluierung psychischer Erkrankungen)? Ist der Entwurf zur Whistleblowing-Betriebsvereinbarung mit den bestehenden Betriebsvereinbarungen im Einklang oder muss angepasst/ nachgebessert werden?

VERHANDLUNGSVORBEREITUNG: FRAGEN AN DIE GESCHÄFTSFÜHRUNG

Sind das Whistleblowing-System und bestehende (Kontroll-)Instrumente im Einklang?

Fügt sich das System in die bestehenden Abläufe im Betrieb ein (evtl. muss man herausfinden, welche Systeme es im Moment schon gibt)? Passt es zu den vorhandenen Betriebsvereinbarungen, die thematisch damit zusammenhängen (ev. eine Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten der Beschäftigten)? Welche anderen Ansprechstellen und workflows gibt es schon im Unternehmen, die damit übereinstimmen müssen (z. B. Interne Revision, compliance officer, Rechtsabteilung) und wie wird das Verhältnis dieser zueinander geregelt?

Welche Themen sollen/können gemeldet werden?

Es gibt theoretisch eine sehr breite Palette an Themen, die in einem betrieblichen Whistleblowing-System gemeldet werden.



Die europäische Richtlinie schränkt den Schutz von WhistleblowerInnen auf **bestimmte Meldeinhalte** ein. Dieser restriktive Zugang zum (arbeits-)rechtlichen Schutz von WhistleblowerInnen setzt sich auch in der nationalen Gesetzgebung (HinweisgeberInnenschutzgesetz) fort.

Siehe Kapitel „Die österreichische Umsetzung der EU-Whistleblowing-Richtlinie“ (Seite 16 f).

Vermutlich wird es sich in der betrieblichen Praxis meist um wirtschaftskriminelle Handlungen bzw. Verstöße gegen Sicherheits- sowie Umwelt- und Gesundheitsregelungen handeln. Die Meldeinhalte sollten jedenfalls konkretisiert werden. Die Gefahr besteht nämlich sonst, dass kleine arbeitsrechtliche Verstöße von MitarbeiterInnen gemeldet werden (z. B. Zu-Spät-Kommen), die eigentlich in den Aufgabenbereich der direkten Führungskraft fallen und nicht in einem Whistleblowing-System behandelt werden sollten. Trotzdem sollte man sich im Klaren darüber sein, dass auch „fremde“ Themen gemeldet werden können – egal wie sie offiziell begrenzt wurden. Wie geht man dann mit einer solchen Meldung im HinweisgeberInnen-System um? Wird sie an den zuständigen Vorgesetzten weitergeleitet? Erfährt der Betriebsrat davon? Wird die Meldung an den/die Meldende/n zurückgeschickt mit dem Verweis, sich an eine andere Stelle zu wenden?

Wer darf das Whistleblowing-System verwenden?

Sollen auch KundInnen/KlientInnen/GeschäftspartnerInnen ausdrücklich aufgefordert werden, Hinweise zu geben? Wie erfahren sie von der Existenz einer Meldestelle? Wie werden sie über allfällig einlangende Meldungen informiert?

Wer ist zuständig für die Bearbeitung und/oder Aufklärung der gemeldeten Missstände?

Da es unterschiedliche Themenkreise gibt, zu denen Meldungen abgegeben werden können, werden unterschiedliche Stellen die weiteren Untersuchungen durchführen. Eine grobe Einteilung, wer wofür zuständig ist, sollte das Ergebnis einer Diskussion im Betrieb zwischen Betriebsrat, Human Resource Management/ Personalabteilung und der Geschäftsführung sein.

Es kommt darauf an, welches Thema gemeldet wurde, ob weitere Personenkreise informiert werden müssen. Beispielsweise muss bei einem Datenleck, das vermutlich durch Hackerangriffe entstanden ist, neben der IT-Abteilung, der/die betriebliche/r Datenschutzbeauftragte informiert werden (so es diese Funktion im Betrieb gibt), in der Regel aber binnen 72 Stunden die Datenschutzbehörde. Ein schwerer Arbeitsunfall wiederum muss innerbetrieblich der Sicherheitsfachkraft und außerbetrieblich der Allgemeinen Unfallversicherungsanstalt (AUVA) und dem Arbeitsinspektorat (AI) bekannt gegeben werden. Um die Zuständigkeiten je

nach beschuldigter Person und Thema darzustellen, kann ein eigener „Bearbeitungspfad“ oder eine „Bearbeitungsmatrix“ erstellt werden.

Es sollte geklärt werden, ob und vor allem mit welcher Genauigkeit eine Information an den Betriebsrat gehen sollte. Manche Gremien finden es ausreichend, wenn sie informiert werden, dass eine Meldung erfolgt ist, möchten aber nicht unnötig in Dinge, die außerhalb ihres Wirkungsbereichs liegen (z. B. Sicherheitsgefährdende Arbeitsbedingungen bei einem ausländischen Zulieferer) involviert werden. Andere Gremien verlangen genaue Angaben zu Art der Verdächtigung, zur Abteilung der der/die Beschuldigte angehört, zum betroffenen Personenkreis, zur Art der ergriffenen Maßnahmen und zum Ergebnis der Untersuchungen, etc.

Wie sieht es mit Melde- und Bearbeitungsfristen aus?

Die EU-Richtlinie sieht vor, dass Meldende (so sie dies wünschen) binnen sieben Tagen den Eingang einer Meldung bestätigt erhalten müssen. Über die ergriffenen Folgemaßnahmen müssen Meldende innerhalb von drei (maximal sechs) Monaten Bescheid erhalten.

Darüber hinaus sollte noch festgelegt werden, nach welcher Zeit das Verfahren eingestellt wird, sollten keine weiteren konkreten Anhaltspunkte/Beweise gefunden werden? Wer entscheidet anhand welcher Kriterien über die Einstellung einer Untersuchung?

Wann werden Meldungen über Vorgänge, die in der Folge nicht bestätigt werden konnten, wieder gelöscht? Was passiert nach der Beendigung bzw. der Einstellung der internen Untersuchungen mit den Unterlagen, die einem Hinweis beigelegt wurden?

Wie ermöglicht man die Anonymität der Beteiligten?

Wie wird mit anonymen Hinweisen umgegangen? Wie wird die Anonymität bzw. der Schutz der HinweisgeberInnen gewährleistet?

Wie werden die Rechte des/der Beschuldigten gewahrt?

Die MitarbeiterInnen brauchen die Möglichkeit, die Meldenden nach näheren Details zu befragen. Wie ist die Rückfragemöglichkeit gestaltet? In welcher Form

können Meldende den weiteren Verlauf ihrer Meldung beobachten (z. B. anonyme Mailbox, die nur zu einem speziellen Fall angelegt wird)?

Wie läuft eine Meldung ab? Wie soll mit einem konkreten Hinweis umgegangen werden?

Wie genau funktioniert das System in technischer Hinsicht? Ist eine **Vorführung** möglich?

Falls ein externer Dienstleister (z. B. eine eigens auf Whistleblowing spezialisierte Firma), das System installiert und (technisch) betreut, sollte der Betriebsrat sich erkundigen, wie der Auftragsverarbeitungsvertrag aussieht. Hat der Anbieter inhaltlichen Zugriff auf die Daten oder nicht? Wann wird gelöscht?

Wo steht der **Server**, auf dem die Meldungen gespeichert werden? Liegt der Standort innerhalb der EU oder in einem US-amerikanischen – dem Privacy Shield unterworfenen – Unternehmen bzw. innerhalb eines sicheren Drittlandes?

Gibt es externe Hilfe?

Was konkret hat der/die BetriebsinhaberIn vor, um dafür zu sorgen, dass das System nicht zum „Verpfeifen“ oder als Instrument zur Befriedigung von Rachegefühlen bei Konflikten im Team genutzt wird? Werden ArbeitspsychologInnen oder Coaches (zumindest bei der Einführung oder den ersten konkreten Fällen) einbezogen? Stehen sie später auf Wunsch für die Beteiligten als Hilfestellung zur Verfügung?



Je konkreter diese Fragen mit der Geschäftsführung im Vorfeld sozialpartnerschaftlich diskutiert werden, umso zielgerichteter und passgenauer kann die betriebliche Regelung gestaltet werden.

DIE EINFÜHRUNG EINES HINWEISGEBERINNEN-SYSTEMS

Die Erfahrung zeigt, dass eine Meldestelle nur dann genutzt wird, wenn Zeit, Energie und vorbereitende Überlegungen in den Einführungsprozess einfließen.

Leider kommt es immer wieder vor, dass nach erfolgreicher technischer Umsetzung und erfolgreicher Verhandlung einer Betriebsvereinbarung die Kraft erschöpft ist und die Einführung vernachlässigt wird. Bekennt sich der Betriebsrat zum System, sollte er hier mit Nachdruck eine gut geplante Einführung verlangen.

Um ein Whistleblowing-System nicht nur technisch einzuführen, sondern im Betrieb auch wirklich zum Leben zu bringen, ist gute Planung notwendig.

Der Betriebsrat hat umfassende Gestaltungsrechte in Zusammenhang mit betrieblichen Whistleblowing-Regelungen und zwar von der Einführung über die Änderung bis zur Abschaffung entsprechender Regelungen. Für die Betriebsratskörperschaft empfiehlt es sich im Einführungsprozess folgende Punkte im Auge zu behalten:

- Lässt sich der Betriebsrat auf eine aktive, gestaltende Rolle ein, so kann das durchaus Nutzen bringen: So kann der Betriebsrat gleich von Beginn an das eigene Beratungs- und Unterstützungsangebot für Hinweisgebende darstellen; auf die Rechte von Meldenden und „Beschuldigten“ und einen sinnvollen Umgang mit Whistleblowing hinweisen und wertvolle inputs für die Interessenvertretungsarbeit wie etwa im Arbeitsschutzausschuss, im Wirtschaftsgespräch oder im Aufsichtsrat, gewinnen.
- In jedem Fall ist zu erwägen, wieviel Zeitressourcen der Betriebsrat in den Verhandlungs- und Einführungsprozess sowie auch in die laufende Kontrolle der vereinbarten Standards investieren kann.

- Gibt es bereits ein bestehendes Compliance-Management-System bzw. eine entsprechende Vereinbarung im Betrieb, so ist der Anpassungsbedarf an die neue Rechtssituation zu klären und die Betriebsvereinbarung ggf. zu adaptieren oder neu auszuverhandeln.

Um das HinweisgeberInnen-System zu einem lebendigen Bestandteil der Betriebskultur zu machen, das den Beschäftigten eine Nutzung in sicherem Rahmen erlaubt, können folgende Schritte helfen

- Abschluss einer Betriebsvereinbarung, die arbeits- und datenschutzrechtliche Standards festlegt.
- Jährliche Evaluierung gemeinsam mit der Unternehmensleitung,
- Halbjährlicher Bericht über das System in der Betriebszeitung/am schwarzen Brett/im Newsletter/am Betriebsratsblog,
- Automatische Benachrichtigung des BR wenn eine Meldung im System eingereicht wurde,
- Regelmäßigen Report über Nutzung und abgeleitete Maßnahmen bei Aufsichtsratssitzungen einfordern; z. B. „Anzahl und Themen der Meldungen an das Whistleblowing-System“.



MUSTER-BETRIEBS- VEREINBARUNG

MUSTER-BETRIEBSVEREINBARUNG FÜR HINWEISGEBERINNEN-SYSTEME

zwischen dem

Unternehmen XY

und dem

Betriebsrat des Unternehmens XY

gemäß § 96a und 97 ArbVG



VORBEMERKUNG

Mustervereinbarungen und Leitfäden können Orientierung geben, sind jedoch nur dann nützlich, wenn sie auf die speziellen betrieblichen Umstände zugeschnitten sind. Wird ein Betriebsvereinbarungsmuster nicht „maßgeschneidert“, gehen schnell wichtige Gestaltungsmöglichkeiten verloren. Aus diesem Grund sind die Regelungen der nachfolgenden Betriebsvereinbarung als Eckpunkte zu verstehen. Sie sollen als Anregungen dienen, um daraus eine zu den Verhältnissen im

eigenen Betrieb optimal passende Vereinbarung zu entwickeln.

Die GPA unterstützt und berät gerne auf diesem Weg!

Hinweis: Die in der Muster-Betriebsvereinbarung **grau hinterlegten Passagen** sind als erläuternde Kommentare zu verstehen oder weisen auf alternative Vorgangsweisen hin.

1. BEGRIFF

Unter Whistleblowing ist die Meldung von gravierenden Missständen oder verbotenen Handlungen im Wirkungsbereich eines Unternehmens zu verstehen. Nicht unter Whistleblowing zu verstehen sind hingegen Anschuldigungen und Diffamierung wider besseren Wissens.

WhistleblowerInnen sind Personen, die auf grobe Missstände bzw. illegale Handlungen hinweisen. Eine Meldung wird von ArbeitnehmerInnen oder anderen Beschäftigten (z. B. PraktikantInnen, Leiharbeitskräften etc.) vorgenommen.

2. ZIELSETZUNGEN

Hinweisgebende werden vor sämtlichen Benachteiligungen, denen sie im Betrieb aufgrund ihrer Meldung ausgesetzt sein könnten, geschützt. Ein wirksamer Schutz der Beschäftigten vor Diskriminierung infolge der Aufdeckung betrieblicher Missstände ist ein wesentliches Anliegen dieser Betriebsvereinbarung. Ebenso soll sichergestellt sein, dass Beschuldigte vor Denunziation geschützt werden.

Anonyme Hinweise müssen möglich, sollen aber nicht der Regelfall sein. Mit dieser Vereinbarung werden Hinweisgebende unter anderem dadurch geschützt, dass ihre Meldung auf eigenen Wunsch anonym bleibt. Es soll ferner sichergestellt werden, dass Hinweisen nachgegangen wird. Maßnahmen zur Bereinigung des Missstandes werden getroffen.

3. GRUNDSÄTZE

Die VertragspartnerInnen halten ausdrücklich fest, dass sämtliche in diesem Zusammenhang erworbenen Informationen einzig und allein zur Klärung des Sachverhaltes, auf den sich die Meldung bezieht, verwendet werden dürfen. Jede andere Nutzung ist ausdrücklich untersagt. Insbesondere ist es untersagt, die Hinweise zu Zwecken der Leistungskontrolle, zur Kontrolle des Freizeitverhaltens oder zum Aufdecken privater Angelegenheiten der ArbeitnehmerInnen, die unabhängig von einem gemeldeten betrieblichen Missstand sind, zu verwenden.

4. GELTUNGSBEREICH

Persönlich:

Diese Betriebsvereinbarung gilt für alle ArbeitnehmerInnen (gemäß § 36 ArbVG), Lehrlinge, HeimarbeiterInnen, PraktikantInnen, überlassene Arbeitskräfte sowie WerkvertragsnehmerInnen.

Sollten Personengruppen im Betrieb beschäftigt sein, die nicht unter den ArbeitnehmerInnenbegriff gemäß § 36 ArbVG fallen, dann sollten diese hier aufgezählt werden. Nachdem das betriebliche Meldesystem weiteren Personengruppen, die mit dem Betrieb verbunden sind, zur Verfügung steht, empfiehlt es sich darauf hinzuweisen – auch wenn der BR diese Personen natürlich nicht vertritt (z. B. KundInnen, KlientInnen, LieferantInnen, Familienangehörige etc.).

Sachlich:

Es kommt das System X zum Einsatz. (Name des Herstellers, Name des Systems)

Verantwortliche Stelle ist XY. (Sollte ein externer Dienstleister das System betreiben, ist er zu benennen.)

5. RECHTSGRUNDLAGEN

Die rechtliche Basis bilden die Mitbestimmungs-Tatbestände des Arbeitsverfassungsgesetzes (gemäß §§ 96, 96a und 97 ArbVG). Außerdem kann man an dieser Stelle auf die Informationsrechte des Betriebsrates aufmerksam machen: §§ 91 und 92 ArbVG. Sowie den Bestimmungen des Bundesgesetzes über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnen-schutzgesetz – HSchG).

6. INHALTE EINER MELDUNG

Über das betriebliche HinweisgeberInnen-System können nur solche Missstände gemeldet werden, die grobe Verstöße gegen geltendes Recht darstellen oder (wirtschafts-)kriminelle Handlungen betreffen. Allgemeine und geringfügige Verstöße gegen unternehmensinterne Verhaltensregeln können nicht über das System gemeldet werden.

Jedenfalls Gegenstand des HinweisgeberInnen-Systems sind Meldungen über Verstöße, die in den „Whistleblowing-Richtlinie“ der Europäischen Union geregelt sind, und folgende Bereiche betreffen:

- öffentliches Auftragswesen,
- Finanzdienstleistungen sowie Verhütung von Geldwäsche und Terrorismusfinanzierung,
- Produktsicherheit und -konformität,
- Verkehrssicherheit,
- Umweltschutz,
- Strahlenschutz und kerntechnische Sicherheit,
- Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz,
- öffentliche Gesundheit,
- Verbraucherschutz,
- Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen
- Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 (StGB)

Darüber hinaus bietet die RL weitere Inhalte, die gemeldet werden können, wie beispielsweise, wenn gegen die finanziellen Interessen der EU verstoßen wird oder gegen Körperschaftssteuer-Vorschriften (siehe Artikel 2 sowie EG 15-20 WB-RL).

Je nach Kerngeschäft des Unternehmens und Branchenzugehörigkeit sind unter Umständen nicht alle in der Richtlinie genannten Meldeinhalte von Relevanz (z. B. Verstöße gegen kerntechnische Sicherheit). Sie müssen in der Betriebsvereinbarung nicht aufgezählt werden.

Es können jedoch Inhalte ergänzt werden, die über die Richtlinie hinausgehen, bei denen man sich im Unternehmen aber einig ist, dass dagegen vorgegangen werden soll (z. B. Diskriminierung von bestimmten Beschäftigtengruppen). Werden solche Ergänzungen vorgenommen, muss man sich bewusst sein, dass Meldende dann nicht unmittelbar von der Europäischen Whistleblowing-Richtlinie und HinweisgeberInnen-schutzgesetz geschützt sind. In diesen Fällen gilt dann ausschließlich der Schutz, der in dieser Betriebsvereinbarung gesichert ist.

Hat ein/e ArbeitnehmerIn Hinweise auf ein schwerwiegendes Fehlverhalten, sollte die Meldung ausschließlich dann erfolgen, wenn ein begründeter Verdacht

besteht und der/die ArbeitnehmerIn nach bestem Wissen und im guten Glauben handelt.

7. EINBRINGEN VON HINWEISEN

Zur Entgegennahme und Bearbeitung vertraulicher bzw. anonymer Hinweise wird ein HinweisgeberInnen-System eingeführt. Eine Beschreibung des Systems ist dieser Betriebsvereinbarung als Anhang beigefügt und Bestandteil der Betriebsvereinbarung.

Die Nutzung des HinweisgeberInnen-Systems schmälert nicht das Recht der ArbeitnehmerInnen, ein internes Beschwerdewesen zu nutzen oder Anfragen, Wünsche, Beschwerden oder Anregungen beim Betriebsrat sowie bei der Geschäftsleitung vorzubringen, ohne dadurch in irgendeiner Form benachteiligt zu werden. Ebenso besteht uneingeschränkt das Recht bei der jeweils zuständigen Behörde oder dem Gericht eine Anzeige einzubringen.

Folgender Meldekanal wurde im Unternehmen X eingerichtet:

Je nach Art der Meldemöglichkeiten ist hier das Zutreffende in die BV zu übernehmen.

Eine schriftliche Meldung kann auf dem Postweg an die Adresse xy oder über einen Beschwerde-Briefkasten am Ort xy eingebracht werden.

UND/ODER

Meldende können Hinweise über die Homepage [\[LINK\]](#) erstatten.

UND/ODER

Der/die HinweisgeberIn hat die Möglichkeit, sich [\[LINK\]](#) im System anzumelden.

Bei dieser Variante muss darauf geachtet werden, dass die Anonymität gewahrt wird und keine IP-Adressen ausgeforscht werden.

UND/ODER

Das System ermöglicht mündliche Meldungen über eine Telefon-Hotline oder ein anderes System für gesprochene Nachrichten.

Bei einem solchen System ist darauf zu achten, dass – auf Wunsch der Meldenden – Anonymität ermöglicht wird (z. B. die Stimme des/der Anrufenden verzerrt wird).

UND

Auf Anfrage des/der HinweisgeberIn können ergänzend physische Zusammenkünfte stattfinden.

8. UMGANG MIT MELDUNGEN

Falls es sich um ein elektronisches System handelt und dieses einen verschlüsselten „Postkasten“ enthält, kann folgende Vereinbarung getroffen werden:

Der/die HinweisgeberIn kann einen – auf Wunsch anonymen – elektronischen Postkasten einrichten, über den die weitere Kommunikation (Nachfragen, Status der Bearbeitung) erfolgt. Der Postkasten ist über Referenznummer/selbst gewähltes Passwort/xxx (je nach Ausgestaltung des Systems ist hier bitte gemäß der Systembeschreibung zu ergänzen bzw. zu streichen) so geschützt, dass nur der/die HinweisgeberIn und die MitarbeiterInnen darauf zugreifen können.

Die eingehenden Meldungen/Nachrichten/Hinweise werden von XY entgegengenommen bzw. bei einem externen Dienstleister: von der Firma ABC

Herr/Frau/divers XY bzw. bei einem externen Dienstleister: von der Firma ABC ist in Angelegenheiten des Whistleblowing-Systems nicht weisungsgebunden gegenüber dem Unternehmen X.

Die Firma ABC ist verpflichtet, sich an den Inhalt dieser BV zu halten.

Die Meldestelle bestätigt innerhalb von sieben Tagen dem/der HinweisgeberIn den Eingang der Meldung.

Es werden Ermittlungen eingeleitet und mit größtmöglicher Vertraulichkeit in möglichst kleinem Personenkreis geführt. Die Ermittlung wird mit jenen Personen im Betrieb durchgeführt, die in jenem Bereich arbeiten, der von der Meldung betroffen ist und von dem anzunehmen ist, dass mit ihnen eine Aufklärung gelingen kann.

In größeren Unternehmen kann dazu auch eine Matrix zur Bearbeitung und Weiterleitung von Informationen erstellt werden. In dieser ist ersichtlich, welche Abteilungen/Bereiche zur Aufklärung welcher Meldungen befugt und geeignet sind. Wenn z. B. Inhalt der Meldung ein systematischer Betrug ist, wendet sich die Meldestelle an die Innenrevision. Sollte es sich bei der Meldung um Geldwäsche handeln, wird die Compliance involviert. Je nachdem, wer in Verdacht steht, werden unterschiedliche Abteilungen zur Aufklärung hinzugezogen. Wird z. B. die lokale Standortleitung eines gravierenden Fehlverhaltens verdächtigt, ist die zentrale Rechtsabteilung zu informieren. Oder es ist der Aufsichtsrat zu benachrichtigen, wenn die verdächtige Person ein Mandat im Aufsichtsrat innehat.

Personen in der Meldestelle sowie zu den Ermittlungen hinzugezogene sind auf ihre strenge Verschwiegenheit hinzuweisen solange die Ermittlungen laufen. Hinweise sind unverzüglich und umfassend aufzuklären und dem/der HinweisgeberIn ist eine Rückmeldung über die gesetzten Ermittlungsschritte zu geben.

Sofern eine Meldung mangels Substanz oder Inhalt nicht weiterzuverfolgen ist, wird diese Entscheidung im 4-Augen-Prinzip getroffen [es sollte angeführt werden, durch wen diese Entscheidung getroffen wird] und dokumentiert. Die Entscheidung, weitere Untersuchungen einzustellen sowie eine entsprechende Begründung ist dem/der Meldenden sowie dem/der Beschuldigten unverzüglich mitzuteilen.

9. SCHUTZ DER MELDENDEN PERSON

Dem/der Meldenden wird strengste Vertraulichkeit zugesichert. Auch eine anonyme Meldung ist möglich. Das HinweisgeberInnen-System ermöglicht es entweder technisch oder organisatorisch mit dem/der HinweisgeberIn zwecks Rückfragen zum vorgebrachten Sachverhalt bzw. zum Plausibilitätscheck in Dialog zu treten (z. B. Einrichtung eines eigens angelegten passwortgeschützten „Briefkastens“).

Jede Form von Repressalien aufgrund einer Meldung ist gegen den/die Hinweisgebende untersagt (siehe Artikel 19 WB-RL und § 20 HSchG).

10. SCHUTZ DER BESCHULDIGTEN PERSON

Ermittlungen aufgrund substantieller Meldungen werden unter Einhaltung größtmöglicher Vertraulichkeit in einem möglichst kleinen Personenkreis geführt. Unverzüglich nach Einlangen einer Meldung und Aufnahme interner Erhebungen, wird der/die Beschuldigte durch die zuständige Abteilung bzw. den/die zuständige/n Vorgesetzte/n über die Existenz und den Inhalt der Meldung schriftlich informiert.

Die beschuldigte Person hat grundsätzlich ein Recht auf Einsichtnahme, Stellungnahme und ggf. Richtigstellung der sie betreffenden personenbezogenen Daten in der Meldung sowie auf Beiziehung eines Betriebsratsmitgliedes ihrer Wahl oder einer anderen Vertrauensperson in jedem Stadium des Verfahrens.

Besteht begründete Gefahr, dass im Falle der Benachrichtigung des/der Beschuldigten die Sachlage nicht ausreichend ermittelt werden kann, wird er/sie erst nach Abschluss der Untersuchungen informiert.

Eine Information unterbleibt zwecks Wahrung des Betriebsfriedens auch dann, wenn bereits im Eingangsstadium entschieden wurde, eine Meldung mangels Substanz nicht weiterzuverfolgen oder eine Meldung abzulehnen, weil sie nicht im Einklang mit den angeführten Meldearten steht (siehe Punkt 9 dieser BV). Nachweislich bewusst falsch erhobene Anschuldigungen können für den/die Meldende/n zu arbeitsrechtlichen Konsequenzen führen.

11. DATENSICHERHEIT UND DATENSCHUTZ

Personen mit Zugriffsberechtigung auf das HinweisgeberInnen-System arbeiten betreffend ihrer Aufgaben im Zusammenhang mit dem Meldesystem unabhängig und sind somit nicht weisungsgebunden. Personen mit Zugriffsberechtigung sind hinsichtlich Systemfunktionalität und Anwendungsgrundsätzen geschult. Insbesondere stellt der/die ArbeitgeberIn nachweislich sicher, dass alle ArbeitnehmerInnen, denen Einsichts- und Bearbeitungsrechte eingeräumt wurden, in geeigneter Form über die umfassende besondere Verschwiegenheitspflicht im Umgang mit den aus dem Whistleblowing-System gewonnenen Informationen in Kenntnis gesetzt wurden.

Zugriffsberechtigten Personen und den in den weiteren Prozess eingebundenen Bearbeitenden darf aus der Ausübung ihrer Tätigkeit kein Nachteil entstehen. Wenn sie Einsicht in Dokumente/Aufzeichnungen/Protokolle

etc. im Zusammenhang mit einem Hinweis verlangen, ist ihnen diese zu gewähren.

Die Auflistung der die Meldung entgegennehmenden BearbeiterInnen mit Zugriffsberechtigungen befindet sich im Anhang zu dieser Betriebsvereinbarung. Eine namentliche Auflistung wird dem Betriebsrat vorgelegt und jede Änderung unverzüglich bekanntgemacht.

Im Falle einer Meldestelle, die von Dritten im Auftrag des Unternehmens betrieben wird, empfehlen wir folgendes: „Wird eine Meldestelle bei Dritten eingerichtet, so ist dem Betriebsrat eine entsprechende Auftragsverarbeitervereinbarung vorzulegen und der Auftragsverarbeiter auf die Einhaltung der Betriebsvereinbarung zu verpflichten.“

Im Falle, dass der Server auf dem die Hinweise verarbeitet werden, im EU-Raum steht, empfiehlt die GPA folgendes: „Die technische Anwendung des HinweisgeberInnen-Systems wird über einen externen Server innerhalb der europäischen Union betrieben und durch die Firma ABC als Auftragsverarbeiter technisch betreut. Ein direkter Zugriff auf den Server durch den/die ArbeitgeberIn ist ausgeschlossen.“

12. INFORMATION UND SCHULUNG

Diese Betriebsvereinbarung wird allen Beschäftigten zugänglich gemacht.

Es empfiehlt sich, konkret anzuführen, wo sie aufliegt; z. B. im BR-Büro, im Intranet...

Die Informations- und Schulungsmaßnahmen für das Whistleblowing-System werden zuvor mit dem Betriebsrat beraten. Art und Umfang des Angebots entsprechen der Funktion und Aufgabenstellung der jeweiligen ArbeitnehmerInnen. Der/die ArbeitgeberIn verpflichtet sich, für alle Beschäftigtengruppen ein geeignetes Schulungsprogramm anzubieten und die entsprechenden Zeitressourcen für die Teilnahme zur Verfügung zu stellen.

13. INFORMATION UND MITWIRKUNG DES BETRIEBSRATES

Der Betriebsrat wird bereits im Vorfeld der Einführung hinzugezogen, um mitzuzusprechen, ob eine Datenverarbeitung, über den gesetzlich geregelt Bereich hinausgeht und somit die Durchführung einer

Datenschutz-Folgenabschätzung (gemäß Art 35 DSGVO) erforderlich ist.

Zur Datenschutz-Folgenabschätzung und vorangehender Schwellenwertanalyse hat die GPA eine eigene Unterlage erstellt, die wir gerne zur Verfügung stellen und zu der wir gerne weitere Beratung anbieten.

Die Geschäftsführung informiert den Betriebsrat regelmäßig (z. B. quartalsweise) über:

- die Anzahl der Meldungen,
- die Art der Meldung,
- das Thema zu dem eine Meldung erfolgt ist,
- die Anzahl der bestätigten Vorwürfe,
- die Anzahl der offensichtlich unbegründeten/ substanzlosen Vorwürfe,
- die getätigten Ermittlungsschritte
- sowie die getroffenen organisatorischen Maßnahmen, um zukünftige Missstände zu vermeiden

Diese im Sinne der Transparenz erstellten Berichte sind anonymisiert und werden sowohl dem Vorstand als auch dem Betriebsrat zur Verfügung gestellt. So vorhanden auch dem Aufsichtsrat

Die nach dem ArbVG bestehenden Informations-, Mitwirkungs- und Interventionsrechte des Betriebsrates bleiben davon unberührt.

Wird ein Ermittlungsverfahren eingeleitet, so ist der Betriebsrat umgehend davon in Kenntnis zu setzen und auf sein Verlangen beizuziehen.

Der Betriebsrat wird über jede geplante substantielle Änderung des HinweisgeberInnen-Systems vor deren Umsetzung informiert. Bei dieser Gelegenheit prüfen beide Seiten, ob die Einhaltung der Bestimmungen dieser Vereinbarung gewährleistet ist. Änderungen, die die Regelungen dieser BV berühren, bzw. Erweiterung des Systems bzw. seiner Funktionalitäten bedürfen der Zustimmung des Betriebsrates.

Zeichnungsbevollmächtigte:

für die Unternehmensleitung

.....

Datum:

Zwecks Überprüfung der technischen Systemfunktionen hat der Betriebsrat das Recht, externe Fachexpertise hinzuzuziehen, wobei die entstehenden Kosten von dem/der ArbeitgeberIn zu tragen sind.

14. EVALUIERUNG

Einmal jährlich beraten Betriebsrat, Geschäftsführung und Meldestelle gemeinsam über die Erfahrungen mit dem Whistleblowing-System, die Anwendung des Systems seitens der Beschäftigten, die Anwendung und Einhaltung der vorliegenden Betriebsvereinbarung sowie allfälligen Änderungsbedarf.

15. INKRAFTTRETEN

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft.

wenn gewünscht: „...und ist zum Zweck der Überprüfung zunächst auf x Monate befristet.“

16. ANHANG

- Systembeschreibung sowie deren Aufbewahrungsort (z. B. Büro der Rechtsabteilung etc.)
- Liste der zugangsberechtigten Personen
- (wenn ausgearbeitet) Matrix zur Bearbeitung und Weiterleitung von Informationen im Zusammenhang mit Meldungen von gravierenden Missständen, Liste jener Personen/ Abteilungen, die in der Folge weiterer Recherchen zum Verdachtsfall eingebunden werden
- Allfälliger Auftragsverarbeitervertrag (gem. DSGVO) mit einem externen Dienstleister

Für den Betriebsrat

.....

ANHANG



CHECKLISTE BETRIEBSVEREINBARUNG

Gestaltung der Melde-Hotline

- sichere Kommunikationsmöglichkeit zwischen meldender Person und Meldestelle (z. B. Postkasten, E-Mail-Adresse, Online-Formular, Telefon, persönliches Treffen)
- Anonymität auf Wunsch zur Verfügung stellen
- Zuständige Stelle bestimmen: intern oder extern; Verschwiegenheit, Unabhängigkeit; Schulung jener Personen, die die Meldestelle betreiben [Achtung! Schweigepflicht von NotarInnen/RechtsanwältInnen bezieht sich nur auf deren MandantInnen, daher bezüglich der Hinweisgebenden extra zu vereinbaren]
- Beschränkung der Themen/Inhalte, die gemeldet werden können
- Vorgehensweise für die Weitergabe der Meldung an Betroffene/Rechtsabteilung/Geschäftsführung/Aufsichtsrat/Behörden
- Sicherheitsmaßnahmen
- Fristen für Rückmeldungen an Hinweisgebende (eine Woche für Empfang der Meldung, zwölf Wochen für Folgemaßnahmen)
- Löschfristen (Empfehlung zwei Monate nach Abschluss der Untersuchung)

konkreter Schutz aller Beteiligten, soweit als möglich;

- Beschränkung des Personenkreises über den gemeldet werden kann
- Schutz des/der gutgläubig Meldenden (z. B. vor Benachteiligung; inkl. allfällig involvierter Verwandter und KollegInnen)
- Schutz des Betroffenen

Einsichts- und Mitwirkungsrechte des BR

- Art und Weise der Information an den BR (pseudonymisiert?)
- Zusammengefasst? Auf wesentliche Aussagen beschränkt? Nur an den Aufsichtsrat?)
- Zeitpunkt (einmal im Quartal? Sofort bei Eingang der Meldung?)

CHECKLISTE FÜR BETRIEBSRÄTINNEN IN DER ZUSAMMENARBEIT MIT HINWEISGEBENDEN KOLLEGINNEN

(überarbeitet, Grundlage mit freundlicher Genehmigung entliehen von Nikolaus Roth, Denkklima e.V.)

Zuhören – Nachfragen – Klarheit schaffen

Nicht an Stelle der Hinweisgebenden agieren, sondern die autonome Entscheidung der/des Hinweisgebenden ermöglichen und sie/ihn dazu stärken.

Hilfe beim **Faktencheck**

Belege zusammentragen, strukturieren und dokumentieren helfen.



Hilfe bei der **Risikoanalyse**

Für wen bestehe das Risiko? für den/die ArbeitgeberIn/die Organisation/persönliches Risiko).

Die besondere psychische Belastung erkennen/realisieren helfen. Fachunterstützung organisieren.

Abwägen der Vor- und Nachteile von internem bzw. externem Whistleblowing.

Was ist der passende Weg? Könnte ich überwiegend persönliche Anliegen auf eine andere Schiene bringen – wenn es „ums Prinzip geht“, um „die schlechte Politik“, persönliche Rache?

Verbündete suchen

- Gewerkschaft kontaktieren und sich fallspezifisch beraten lassen;
- Beim Zugang zu anderen Wegen helfen (Internes Beschwerdewesen, innerbetriebliche oder externe Hilfsangebote).
- Kontakt zu Verantwortlichen oder SpezialistInnen vermitteln.
- Prüfen, ob der sachliche Kern der Information über VertreterInnen / Betriebsrat vorgebracht werden sollte.
- AnsprechpartnerInnen (ev. auch betriebsexterne Hilfe/ Meldestelle/ Behörde) suchen helfen.

bei Bedarf: **Rechtsschutz** organisieren

CHECKLISTE FÜR HINWEISGEBENDE ARBEITNEHMERINNEN

(überarbeitet, Grundlage mit freundlicher Genehmigung entliehen von Nikolaus Roth, Denkklima e.V.)

Kenne ich den **Sachverhalt** zur Gänze?

- Belege/Beweise/Rechnungen/Schriftstücke/E-Mails/Fotos/(Gedächtnis-)Protokolle/Telefonnotizen sammeln und dokumentieren.
- Branchenspezifische/arbeitsrechtliche/betriebsinterne Regeln und Abläufe kennen und – nach Möglichkeit – beachten.
- AnsprechpartnerInnen suchen.

Zur allfällig erforderlichen Klärung des Sachverhalts

- Welche **Gefahren** drohen aus dem beobachteten Sachverhalt? Und wem?
- Welche **Auswirkungen** des Fehlverhaltens für das Unternehmen sind besonders wahrscheinlich, welche besonders schwerwiegend? Habe ich verstanden, warum sich die Verantwortlichen so verhalten? Kennen die Beteiligten das Risiko und nehmen es – bewusst – in Kauf?
- Welche Auswirkungen könnte das Whistleblowing auf mich haben?
- Könnte ich persönliche Anliegen auf eine andere Schiene bringen – wenn es „ums Prinzip geht“, um „die Politik“, persönliche Rache oder Kritik an Managemententscheidungen?

ÖFFENTLICHE MELDESTELLEN IN ÖSTERREICH

Es sind zu unterschiedlichen Themen öffentlich zugängliche Meldesysteme eingerichtet. An diese können sich HinweisgeberInnen – egal ob ArbeitnehmerIn, Selbständige/r PensionistIn oder SchülerIn – wenden um problematische Beobachtungen und Sachverhalte zu melden.

- Seit März 2013 hat das Justizministerium ein Hinweisgebersystem (BKMS-System) bei der Zentralen Staatsanwaltschaft zur **Verfolgung von Wirtschaftsstrafsachen und Korruption** eingerichtet.
 <https://www.bkms-system.net/wksta>
- Im Bundesministerium für Inneres werden **Verdachtsfälle bei Drogen-, Umwelt- oder Internetkriminalität** jeder Art entgegengenommen.
 <https://bundeskriminalamt.at/602/start.aspx>
- Bei der NGO ZARA, für Zivilcourage und Antirassismus-Arbeit betreibt eine **Meldestelle gegen Rassismus und eine gegen Hass im Netz**.
 <https://zara.or.at/de/beratungsstellen>
- Bei der Internetserviceprovidern Österreichs (ISPA) können Fälle von **Kinderpornografie** und **nationalsozialistische Wiederbetätigung im Internet** gemeldet werden.
 <https://www.stopline.at/de/melden>
- Im Whistleblowing-System der Bundeswettbewerbsbehörde können Kenntnisse eines **wettbewerbswidrigen Verstoßes** (etwa eines **Kartelles oder Marktmachtmissbrauches**) gemeldet werden.
 <https://report.whistleb.com/de/bwb>
- Kenntnis von **Misständen oder Verstößen gegen Aufsichtsrecht** in einer Organisation können im Hinweissystem der FMA abgegeben werden.
 <https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=11FMA61&c=-1&language=ger>

STICHWORTVERZEICHNIS

ArbeitspsychologInnen	30
Aufsichtsratssitzung	31
Auftragsverarbeitungsvertrag	30
Bearbeitungsmatrix	30
Betriebskultur	31
Betriebsratskörperschaft	28
Compliance	10
Datenerfassung, automationsunterstützte	20
Datenschutz-Folgenabschätzung	26
Datenverarbeitung, automationsunterstützte	20
Datenweitergabe, automationsunterstützte	20
Diskriminierung	13
Disziplinarmaßnahmen	13
Einführung, -prozess, -planung	30
Enron	9
EU-Richtlinie	12
Europäische Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (2018/0106 (COD))	11
Evaluierung	31
Frist, Melde-, Bearbeitungs-	12, 15, 30,
Geheimnisverrat	24
Geltungsbeginn	12
Geschäftsgeheimnis	24
Gewerkschaften	14
Implementierung	30
Kontrollmaßnahmen, -systeme	18, 20
Kündigung	13
Meldeinhalt	12, 16, 29
Meldekanal	14
Meldestelle, Pflicht	13
Meldestelle, Einrichtungspflicht	14
Meldethemen	12, 29
Mobbing	13
Muster-Betriebsvereinbarung	32
Nationales Recht	13
öffentliches Interesse	8
Ordnungsvorschrift, betriebliche	20
Personenkreis, geschützter	12
Prozessablauf	29
Rahmenbetriebsvereinbarung	29
Sarbanes-Oxley-Act, SOX	10, 25
Schutz, der Anonymität	30
Schwarze Liste	13
Schwellenwertanalyse	27
Treuepflicht	23
Überwachung von ArbeitnehmerInnen	20
Umsetzung der WB-RL	13
Verfahren	29
Verhaltensrichtlinien, Verhaltenskodex, Ethik-Charta, Code of Conduct, Compliance Policy,	23, 24, 25
Zugang, leicht zugänglich	14
Zuständigkeit	29
Whistleblowing-Richtlinie (WB-RL)	11 ff.
Verbotene Repressalien	13
Betriebsvereinbarung	15, 32 ff.
HinweisgeberInnenschutzgesetz (HSchG)	16
Beweislastumkehr	17
Sanktionen	17
Meldepflicht	22
Verschwiegenheitspflicht	23
Verarbeitungsverzeichnis	27
Verhandlungsvorbereitung	29

**GEWERKSCHAFT GPA
IN GANZ ÖSTERREICH**

**SERVICE-HOTLINE:
+43 (0)5 0301**

GEWERKSCHAFT GPA

Service-Center

1030 Wien, Alfred-Dallinger-Platz 1

Tel.: +43 (0)5 0301

Fax: +43 (0)5 0301-300

E-Mail: service@gpa.at

GPA Wien

1030 Wien, Alfred-Dallinger-Platz 1

GPA Niederösterreich

3100 St. Pölten, Gewerkschaftsplatz 1

GPA Burgenland

7000 Eisenstadt, Wiener Straße 7

GPA Steiermark

8020 Graz, Karl-Morre-Straße 32

GPA Kärnten

9020 Klagenfurt, Bahnhofstraße 44/4

GPA Oberösterreich

4020 Linz, Volksgartenstraße 40

GPA Salzburg

5020 Salzburg,
Markus-Sittikus-Straße 10

GPA Tirol

6020 Innsbruck,
Südtiroler Platz 14

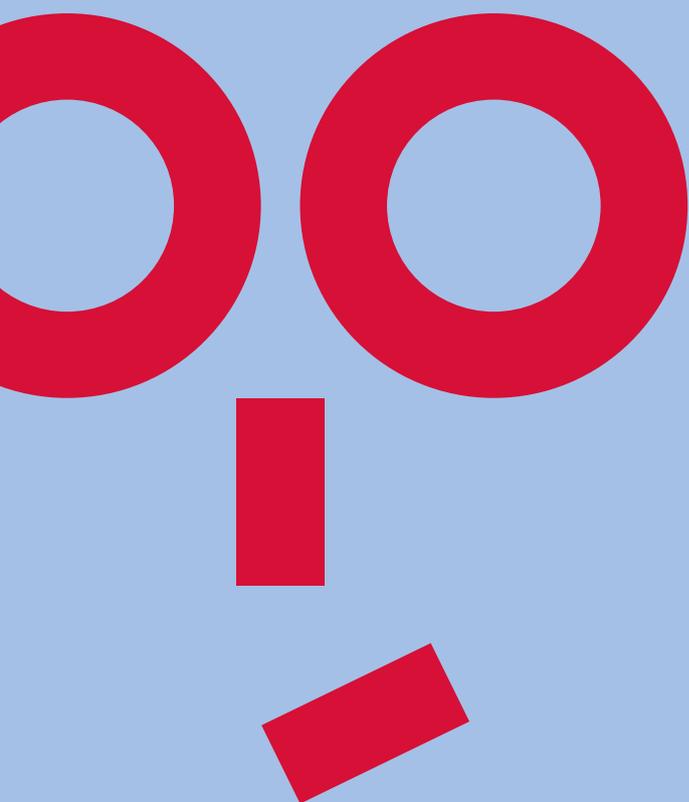
GPA Vorarlberg

6900 Bregenz, Reutegasse 11



www.gpa.at

**OO GUTE
ARBEIT!**



mitgliedwerden.gpa.at

