Datenschutzrechtliche Aspekte bei der Umsetzung der Whistleblower-Richtlinie in Unternehmen

Lucia Neumayer

§ 1 Einführung: Definition

Der Begriff ‚*Whistleblower*' lässt sich von der englischen Redewendung ‚to blow the whistle' ableiten und bedeutet übersetzt so viel wie ‚in die Pfeife blasen'. Im deutschen Sprachraum ist damit ein ‚Enthüller' oder ‚Hinweisgeber' gemeint, der Informationen aus einem vertraulichen oder geheimen Umfeld an die Öffentlichkeit bringt, da diese von allgemeinem Interesse sind. Diese Meldungen betreffen meist Missstände wie Insiderhandel, Korruption oder Datenmissbrauch und verweisen auf Vorgänge in der Politik, in Behörden oder privatwirtschaftlichen Unternehmen. Im beruflichen Kontext schwingt hier oft auch ein negativer Beigeschmack des Denunzierens, ‚Verpetzens' oder ‚Anlastens' mit. Personen wie Julian Assange, der Gründer von WikiLeaks, sowie Edward Snowden, der einen der größten Datenschutzskandale der US-Geschichte mit der Veröffentlichung des PRISM-Überwachungsprogramms der National Security Agency (NSA) auslöste, sind mittlerweile weltweit bekannt und gaben dem Terminus ‚Whistleblower' ein Gesicht.[1]

Bei der Beschäftigung mit Hinweisgebern und deren gesetzlichen Schutz ist ein Blick in die USA unvermeidlich. Der Schutz von Whistleblowern wurde dort im Wesentlichen von drei Bundesgesetzen geformt.

1863 war es der US-Präsident Abraham Lincoln, der mit dem ‚US False Claims Act'[2] die erste Whistleblowing-Bestimmung erließ. Diese Regelung gab Privatpersonen, die im Auftrag des Staates eine Klage einbrachten, einen Anspruch auf einen Teil des Schadenersatzes. In den Vereinigten Staaten ist Whistleblowing daher bereits ein in der Gesellschaft verankertes Instrument zur Aufdeckung von Verbrechen oder Missständen.

1 Ehrbar NetV 2016, 20 (20).

2 United States Department of Justice, The False Claims Act, abrufbar unter: https://www.justice.gov/civil/false-claims-act (Stand 15.12.2023).

Im Jahr 2001 wurde – als Reaktion auf die Bilanzskandale des Energiekonzerns ENRON sowie des Telefonkonzerns WorldCom – der ‚Sarbanes-Oxley Act'[3] (SOX) erlassen.[4] Somit wurden alle US-börsennotierten Unternehmen zur Implementierung von unternehmensinternen Whistleblowing-Hotlines verpflichtet. Auf Grund der exterritorialen Wirkung des SOX sind davon auch ausländische Unternehmen betroffen, wenn deren Aktien an der US-Börse gehandelt werden.[5] Mit der Schaffung des ‚Dodd-Frank Wall Street Reform and Consumer Protection Act'[6], der in Folge der Auswirkungen der Finanzmarktkrise 2007 ein Belohnungssystem für Meldungen von Verstößen gegen US-Wertpapiergesetze etablierte, ging folgende Änderung einher: Whistleblower erhalten seither bei Hinweisen zu Verstößen gegen das amerikanische Wertpapiergesetz einen Teil der Schadenssumme als Belohnung.[7]

Der Begriff ‚Whistleblowing' hat in den letzten zehn Jahren aber auch im öffentlichen Diskurs in Europa stark an Bedeutung gewonnen.[8] Einer der wohl bekanntesten Whistleblower ist Edward Snowden, ein ehemaliger Mitarbeiter der CIA, dem amerikanischen Geheimdienst. Er veröffentlichte im Sommer 2013 geheime Dokumente aus dem PRISM-Programm der National Security Agency (NSA) zur weltweiten Internetüberwachung durch den US-Militärgeheimdienst. Den Hinweis gab er erst anonym, später legte er seine Identität aber offen, weil er sich dadurch mehr Schutz vor den Strafverfolgungen durch die US-Regierung erhoffte. Aufgrund der internationalen medialen Berichterstattung der NSA-Affäre geriet auch Snowden in den Fokus der breiten Öffentlichkeit.[9] Ein weiterer Whistleblower, der mit der Veröffentlichung und Aufklärung von Missständen in amerikanischen Behörden weltweite Bekanntheit erlangte, ist Julian Assange, der Gründer von Wikileaks. Im Sommer 2022 beschloss die Regierung Groß-

3 Vgl. dazu https://www.congress.gov/bill/107th-congress/house-bill/3763/text/enr (Stand 15.12.2023).
4 *Fidler/Winner* in *Kalss/Oppitz/U. Torggler/Winner*, BörseG/MAR § 124 BörseG Rn. 41.
5 Pollirer Dako 2020, 38 (38).
6 https://www.congress.gov/bill/111th-congress/house-bill/4173 (Stand 07.12.2023).
7 *Fleischer/Schmolke* NZG, 361 (368).
8 Hastenrath CB 2022, 58 (58).
9 Ehrbar NetV 2016, 20 (20).

britanniens jedoch, ihn an die Vereinigten Staaten auszuliefern, wo ihm ein Prozess wegen Spionagevorwürfen droht.[10]

Bei diesen Beispielen handelt es sich zwar um besonders schwere Skandale, die aufgedeckt wurden, jedoch nicht um Einzelfälle. Durch den unzureichenden Schutz und die daraus resultierenden teils lebenslangen Nachteile durch die Offenlegung von rechtswidrigen Praxen oder geheimen Unterlagen könnten potenzielle Hinweisgeber jedoch abgeschreckt werden. In Österreich, aber auch in den meisten anderen Mitgliedsstaaten der europäischen Union ist der rechtliche Schutz von Whistleblowern bisher nur unzureichend vorhanden gewesen. Genau dies soll sich mit der EU-Richtlinie zum Hinweisgeberschutz künftig ändern.[11]

§ 2 Tätigwerden der Kommission

Das Ziel der Erarbeitung einer Richtlinie zum unionsweit einheitlichen Schutz von Whistleblowern verfolgte die Europäische Kommission bereits seit 2017. Zu diesem Zeitpunkt hatten nur zehn Mitgliedstaaten einen ausreichenden Schutz für Hinweisgeber gesetzlich verankert. Dazu gehörten: Irland, Italien, Litauen, Malta, die Niederlande, Schweden, die Slowakei, Ungarn und das Vereinigte Königreich. Die anderen Staaten sahen nur teilweise Schutzmechanismen vor bzw. schützten nur bestimmte Gruppen.[12] Am 16.12.2019 trat dann die finale EU-Richtlinie zum Hinweisgeberschutz gem. RL (EU) 2019/1937 in Geltung, die sogenannte Whistleblower-Richtlinie (WBRL).

Bis zu diesem Zeitpunkt war die Erarbeitung der Richtlinie jedoch stark von politischen Auseinandersetzungen umkämpft.[13] Das Drängen zu einer umfassenden Regelung zum unionsweiten Hinweisgeberschutz ging nicht von der Kommission, sondern vom Europäischen Parlament aus. Mit seinen beiden Entschließungen[14] war das Parlament die treibende Kraft, die die Kommission zur Erarbeitung eines Gesetzgebungsvorschlags für einen umfassenden, unionsweiten Schutz von Whistleblowern aufforderte. Am

10 tagesschau, Gründer von WikiLeaks: London bestätigt Auslieferung von Assange an die USA (Stand: 17.06.2022) Vgl. dazu https://www.tagesschau.de/ausland/europa/auslieferung-assange-107.html.
11 Teichmann/Weber CB 2022, 157 (157).
12 Peitsch NetV, 60 (60).
13 Schmolke NZG 2020, 5 (5).
14 2016/2055(INI)); (2016/2224(INI)).

23.4.2018 wurde sodann der erste Vorschlag zur Richtlinie vorgelegt.[15] Dieser war inhaltlich an die Empfehlungen des Europarates zum Schutz von Whistleblowern angelehnt.[16]

Eine von der Europäischen Kommission in Auftrag gegebene Studie im Zuge der Erarbeitung der Richtlinie geht bezüglich der jährlichen Einnahmeausfälle auf EU-Ebene durch Korruption und Betrug von 179 bis 256 Milliarden Euro aus.[17] Nur im Bereich des öffentlichen Auftragswesens sind die Ertragsausfälle, wegen eines nicht ausreichenden Schutzes von Hinweisgebern, jährlich auf 5,8 bis 9,6 Milliarden Euro zu schätzen.[18]

Der erste Vorschlag war dem Europäischen Parlament aber nicht weitreichend genug. Der zuständige Rechtsausschuss legte in einer Entschließung des Parlaments legislative Änderungen vor, die den Schutz der möglichen Hinweisgeber in weitgehender Weise gewährleisten sollte. Zu den umstrittensten Punkten zählten das dreigliedrige Meldesystem (interne Meldung, externe Meldung und Offenlegung) sowie der Schutz von anonymen Hinweisgebern, die erst später identifiziert werden, und der Schutz von Personen, die den Hinweisgeber unterstützen (‚Mittler').[19]

Mitte März des Jahres 2019 gelang es dem Rat und dem Parlament, sich schließlich über die neue Richtlinie zu einigen. Im April des gleichen Jahres gab dann das Parlament seine Zustimmung, im Oktober schließlich auch der Rat. Am 26.11.2019 wurde die EU-Richtlinie dann im Amtsblatt veröffentlicht. Sie ist seit Dezember 2019 in Kraft.

§ 3 Die Whistleblower-Richtlinie

Die Mitgliedstaaten hatten mit einer Frist bis zum 17.12.2021 Zeit, um die neuen Vorgaben der Richtlinie in nationales Recht nach RL (EU) 2019/1937 umzusetzen. Die Realisierung in Österreich erfolgte jedoch nicht fristgerecht, weshalb im Jänner 2022 ein Vertragsverletzungsverfahren durch die Kommission gegen die Republik Österreich eingeleitet wurde.[20] Der erste

15 COM(2018) 218 final.
16 CM/Rec (2014)7).
17 COM(2018) 218 final, 11.
18 COM(2018) 218 final, 3.
19 COM(2018)0218 – C8-0159/2018 – 2018/0106(COD).
20 INFR(2022)0004.

Entwurf zur Umsetzung wurde mit einer Begutachtungsfrist vom 03.6.2022 bis zum 15.7.2022 vom Arbeitsministerium veröffentlicht.[21]

Am 25.02.2023 trat das HinweisgeberInnenschutzgesetz (HSchG)[22] in Österreich schlussendlich in Kraft. Mit über einem Jahr Verspätung wurde damit die WBRL in innerstaatliches Recht umgesetzt.[23]

Im folgenden Kapitel werden die relevantesten Inhalte der Richtlinie näher beleuchtet. Der wesentliche Fokus liegt hierbei auf der datenschutzrechtlichen Umsetzung der WBRL in Unternehmen unter Bezugnahme auf das österreichische Gesetzt, zur Umsetzung der Richtlinie sowie dessen Begutachtungsverfahren.

A. Inhalt und Zweck der Richtlinie

Der Art. 1 der Richtlinie steckt die Ziele der WBRL ab: Diese liegen gem. Art. 1 WBRL in erster Linie darin, die bessere Durchsetzung von Unionsrecht zu gewährleisten sowie das Schutzniveau für Whistleblower zu vereinheitlichen und zu erhöhen.

Der vorgesehene Schutz vor Repressalien soll Beschäftigte gem. Erwgr. 1 WBRL von privaten sowie öffentlichen Organisationen dazu ermutigen, Gesetzesverstöße zu melden, die das öffentliche Interesse betreffen.

B. Anwendungsbereich

I. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich der WBRL wird in Art. 4 WBRL weit gefasst, damit möglichst alle Personen, die Informationen über Verstöße offenlegen möchten, ebenfalls geschützt sind.

Vom persönlichen Anwendungsbereich der Richtlinie umfasst werden daher alle Arbeitnehmer, die in den unionsrechtlichen Arbeitnehmerbegriff nach Art. 45 Abs.1 Vertrag über die Arbeitsweise der Europäischen Union fallen. Im Erwägungsgrund 38 zur WBRL wird außerdem festgehalten, dass diese sowohl Personen „*in atypischen Beschäftigungsverhältnissen, Teilzeitbeschäftigte, Personen in befristeten Beschäftigungsverhältnissen und*

21 ME HSchG 2022, 210/ME 27. GP.
22 ÖBGBl. 2023 I 6.
23 Irresberger/Stangl-Krieger/Bruchbacher/Kercz/Wasinger GRCaktuell 2023, 28.

Leiharbeiter" (Erwgr. 38 WBRL) einschließt als auch für Beamte und Vertragsbedienstete im öffentlichen Dienst gelte. Erfasst sind darüber hinaus ehemalige sowie künftige Beschäftigte.

Neben den Arbeitnehmern werden vom persönlichen Anwendungsbereich auch Selbständige gem. Art. 49 AEUV sowie Anteilseigner und Personen eingeschlossen, die dem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören. Des Weiteren sind ebenfalls Berater, Auftraggeber und Lieferanten geschützt.

Aber nicht nur die Person des Hinweisgebers ist abgesichert, vielmehr gilt dies gleichermaßen für natürliche Personen, die den Hinweisgeber unterstützen oder ermutigen, den Hinweis abzugeben, natürliche Personen, die dem Hinweisgeber nahestehen und dadurch auch von Repressalien betroffen sein könnten, wie etwa Kollegen oder Verwandte, sowie des Weiteren ebenfalls juristische Personen, die im Eigentum des Hinweisgebers sind oder für die er arbeitet, so gem. Art. 4 WBRL .

II. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich erstreckt sich auf Verstöße gegen das Unionsrecht, die in eine der im Anhang zur Richtlinie angeführten Unionsrechtsakte der Union fallen und in Art. 2 Abs. 1 lit. a WBRL enumerativ aufgelistet sind. Dazu gehören das öffentliche Auftragswesen, Finanzdienstleistungen, Geldwäsche, Terrorismusfinanzierung, Verkehrssicherheit, Umweltschutz, Produktsicherheit, Verbraucherschutz und Datenschutz.

Die Legaldefinition des ‚Verstoßes' findet sich in Art. 5 Ziff. 1 WBRL. Davon umfasst werden rechtwidrige Handlungen sowie Unterlassungen gegen die in Art. 2 WBRL angeführten Rechtsgebiete wie in Art. 5 Z1 WBRL ausgeführt.

Nicht eingeschlossen ist ein unethisches, dem öffentlichen Interesse widerstrebendes Verhalten.[24]

Explizite Ausnahmen des sachlichen Anwendungsbereichs finden sich in Art. 3 Abs. 2–4 WBRL. Dazu zählen etwa Angelegenheiten der nationalen Sicherheit, der Schutz von Verschlusssachen oder jener der anwaltlichen und ärztlichen Verschwiegenheitspflicht, wenn sie durch einen Mandanten oder Patienten einen Verstoß erfahren.

24 Schmolke NZG 2020, 5 (6).

Dies bedeutet aber auch, dass Fälle wie jener von Edward Snowden nicht in den Anwendungsbereich der WBRL fallen würden.[25]

Die Richtlinie gibt den Mitgliedstaaten darüber hinaus die Befugnis, den sachlichen Anwendungsbereich ebenfalls auf Bereiche des jeweiligen nationalen Rechts zu erweitern, so geregelt in Art. 2 WBRL. Eine Ausdehnung auf Verstöße gegen das nationale Recht hätte auf der einen Seite den Vorteil, dass der Hinweisgeber vor der Meldung nicht erst kontrollieren muss, ob der Verstoß tatsächlich europäisches und nicht innerstaatliches Recht betrifft. Eine solche Prüfung wird den Rechtsunterworfenen in vielen Fällen nicht zumutbar sein.[26] Dies kann außerdem dazu führen, dass der Whistleblower seine Meldung aus Angst, doch nicht geschützt zu sein, schlichtweg unterlässt.[27] Auf der anderen Seite trifft dies auch auf die Meldestellen zu, da diese nach Eingang einer Meldung ebenso erst feststellen müssen, ob ein Verstoß gegen das Unionsrecht vorliegt.[28]

C. Das Meldesystem

Die Ausgestaltung und die Umsetzung des Meldesystems gehörten bei der Entstehung der WBRL wohl zu den essenziellsten Streitgegenständen. Erst war die Ausgestaltung als ein dreistufiges System mit den Stufen intern – extern – öffentlich geplant. Letzten Endes wurde jedoch die Entscheidung für ein zweistufiges System getroffen. Die Richtlinie sieht nun ein Meldesystem mit einem internen und einem externen Meldekanal vor und erst danach steht dem Hinweisgeber die Möglichkeit der Offenlegung frei.[29]

In Art. 7 Abs. 2 WBRL wird eindeutig festgehalten, dass die Staaten bei der Umsetzung der Richtlinie in nationales Recht sich verstärkt für interne anstatt externe Meldekanäle einsetzen sollen, wenn dadurch die Wirksamkeit des Vorgehens gegen den gemeldeten Verstoß höher ist und der Hinweisgeber keine Repressalien fürchten muss.

Für Hinweisgeber muss es gem. Art. 9 Abs. 2, Art. 12 Abs. 2 WBRL möglich sein, einen Verstoß sowohl mündlich als auch schriftlich oder durch ein persönliches Treffen zu melden. Dem Whistleblower muss nach der

25 Schmolke NZG 2020, 5 (8).
26 Arnold GesRZ 2020, 153 (154).
27 Kröll/Stumpf RdW 2020, 161 (162).
28 *Falter*, Whistleblower (un)erwünscht? in *Roters/Gräf/Wollmann* (Hrsg), Zukunft Denken und Verantworten (2020) 353 (366).
29 Reppelmund EuZW 2019, 307.

Meldung innerhalb von sieben Tagen eine Bestätigung des Eingangs zugehen. In weiterer Folge muss ihm innerhalb von drei Monaten (in besonderen Fällen sechs Monaten) nach Erhalt der Eingangsbestätigung Rückmeldung über den Stand der Meldung und Folgemaßnahmen erstattet werden, so geregelt in Art. 9 Abs. 1 lit. f WBRL. Zu Letzteren zählen die Schlüssigkeitsprüfung der Hinweise und in weiterer Folge die Einleitung von Ermittlungen, Strafverfolgungsmaßnahmen oder der Abschluss des Verfahrens wie in Art. 5 Ziff. 12 WBRL festgesetzt.

I. Interne Meldekanäle

Mit der Umsetzung der Richtlinie in nationales Recht haben die Mitgliedsstaaten für die Errichtung von internen Kanälen zur Meldung und für verfahrensgerechte Folgemaßnahmen zu sorgen. Meldekanäle sind gem. Art. 8 Abs. 1 WBRL gleichermaßen bei juristischen Personen sowohl im privaten als auch im öffentlichen Sektor einzurichten, was im Einklang mit den Sozialpartnern geschehen sollte.

Von der Pflicht der Errichtung sind juristische Personen des Privatrechts ab 50 Arbeitnehmern betroffen. Unabhängig davon sind nach Art. 8 Abs. 4 WBRL ebenso juristische Personen zur Einrichtung eines Meldekanals verpflichtet, auf die die im Anhang in den Teilen I. B sowie II angeführten Unionsrechtsakten einschlägig sind. Hierbei geht es um Akte des Finanzsektors, der Verhinderung von Geldwäsche und der Bekämpfung von Terrorismus, der Verkehrssicherheit und des Umweltschutzes.[30]

Darüber hinaus besteht für die Mitgliedstaaten gem. Abs. 7 WBRL die Möglichkeit der Mitgliedstaaten, nach Durchführung einer geeigneten Risikobewertung zugleich juristische Personen mit weniger als 50 Arbeitnehmern zur Errichtung von Meldekanälen und Verfahren zu verpflichten. Die Betriebe werden dabei auf ein bestehendes Risiko für die Umwelt oder die öffentliche Gesundheit überprüft. Davon sind Unternehmen betroffen, die insbesondere in den Sektoren der Lebensmittelindustrie, der Pharmazie, der Chemie oder dem Baugewerbe tätig sind.[31] Trifft ein Mitgliedsstaat eine solche Entscheidung, so hat er dies gem. Art. 8 Abs. 8 WBRL der Kommission mitzuteilen, die die anderen Mitgliedsstaaten darüber informieren wird.

30 Novacek FJ 2019, 222 (223).
31 Kröll/Stumpf RdW 2020, 161 (162).

Außerdem sind auch juristische Personen des öffentlichen Rechts von der Pflicht zur Errichtung interner Meldekanäle betroffen. Eine Mitarbeitergrenze wie bei juristischen Personen des privaten Sektors ist hier nicht vorgesehen. Die Richtlinie gibt den Mitgliedstaaten den Handlungsspielraum, Gemeinden mit weniger als 10.000 Einwohnern oder weniger als 50 Arbeitnehmern von der Pflicht zur Implementierung interner Meldekanäle ausnehmen zu können, so geregelt in Art. 8 Abs. 9 WBRL.

Die Art des Meldekanals, der eingerichtet werden muss, unterliegt gem. Art. 8 Abs. 5 WBRL der Entscheidung der juristischen Person des Privatrechts bzw. des öffentlichen Rechts selbst. Zudem muss der Meldekanal nicht im Unternehmen intern betrieben werden, sondern kann ebenfalls an Dritte ausgelagert werden, die damit beauftragt werden, das Hinweisgebersystem für das Unternehmen zu betreiben. Im Erwägungsgrund 53 der Richtlinie werden Beispiele für interne Meldekanäle genannt. Diese können gem. Erwgr. 53 WBRL unter anderem sein: ein Beschwerde-Briefkasten, eine Plattform im Intra- oder Internet oder eine Telefonhotline. Da neben den Beschäftigten aber auch dritte Personen wie Lieferanten oder Subunternehmen in den persönlichen Anwendungsbereich der WBRL fallen und demnach einen Hinweis abgeben können, muss der interne Meldekanal auch für unternehmensfremde Person geöffnet und zugänglich sein.

Das Betreiben der internen Meldestelle muss gem. Erwgr. 54 WBRL nicht durch die juristische Person selbst erfolgen, sondern ist ebenso durch Dritte möglich, wie externe Berater, Prüfer oder spezielle Anbieter von Meldeplattformen sowie Arbeitnehmer- und Gewerkschaftsvertreter. Essenziell ist, dass die Vertraulichkeit und die Identität des Hinweisgebers gewahrt bleiben.

II. Externe Meldekanäle

Grundsätzlich steht es den Hinweisgebern frei, die Meldung an eine interne oder externe Meldestelle zu erstatten. Die Richtlinie hält in Art. 7 Abs. 2 WBRL die Mitgliedsstaaten jedoch dazu an, interne Meldekanäle zu priorisieren.

Behörden sollen von den Mitgliedstaaten als externe Meldestellen benannt und für die Einrichtung einer unabhängigen und autonom handelnden externen Meldestelle sowie für das Setzen geeigneter Folgemaßnahmen zuständig werden. Im Erwägungsgrund 64 werden entsprechende Behörden genannt, die hierfür in Betracht gezogen werden können: Justiz- oder Strafverfolgungsbehörden, Regulierungs- und Aufsichtsstellen, Stellen zur

Korruptionsbekämpfung oder Ombudspersonen, - so geregelt in Erwgr. 64 WBRL.

Bei externen Meldekanälen gelten gem. Art. 11 Abs. 2 lit. b WBRL die gleichen Fristen zur Verständigung von Whistleblowern wie bei internen Kanälen: Innerhalb von sieben Tagen nach einer Meldung muss eine Eingangsbestätigung erfolgen. Nach drei Monaten sowie in besonderen Fällen nach sechs Monaten hat dann gem. Art. 11 Abs. 2 lit. d WBRL die Rückmeldung über den Stand der Meldung und Folgemaßnahmen zu erfolgen. Nach Ende der Ermittlungstätigkeit muss ihm dann gem. Art. 11 Abs. 2 lit. e WBRL ein endgültiges Ergebnis mitgeteilt werden. Speziell geschulte Mitarbeiter der externen Meldestelle sind laut Art. 12 Abs. 4 - 5 WBRL für die Entgegennahme der Meldung, die Einleitung von Folgemaßnahmen und die Kommunikation mit dem Hinweisgeber zuständig. Sollten Mitarbeiter die Meldung auf anderem Weg als über den Meldekanal erhalten, so ist gem. es ihnen Art. 12 Abs. 3 WBRL untersagt, Informationen offenzulegen, durch die die Geheimhaltung der Identität des Hinweisgebers gefährdet werden könnte.

Wird eine Meldung an eine unzuständige Behörde erstattet, so ist diese Behörde verpflichtet, unter Inkenntnissetzung des Hinweisgebers, die Meldung an die jeweils zuständige Behörde weiterzuleiten. Wird es durch das nationale Recht oder das Unionsrecht vorgesehen, so haben die Behörden gem. Erwgr. 71 WBRL darüber hinaus eine Übermittlung der Meldung an die zuständigen Stellen der Union durchzuführen, etwa an das Europäische Amt für Betrugsbekämpfung oder die Europäische Staatsanwaltschaft.

In Art. 13 WBRL heißt es weiters, dass die Behörden leicht verständliche und zugängliche Informationen über die Entgegennahme von Hinweisen und die Vorgehensweise bezüglich Folgemaßnahmen auf ihrer Website zu veröffentlichen haben.

III. Offenlegung

Die Offenlegung ist die letzte Stufe des Meldesystems. Unter einer ‚Offenlegung' versteht die Richtlinie „*das öffentliche Zugänglichmachen von Informationen über Verstöße*" (Art. 5 Ziff. 6 WBRL). Der Weg der Offenlegung nach Art. 15 WBRL steht dem Hinweisgeber jedoch nur frei, wenn einer der folgenden Fälle vorliegt: Die Meldungserstattung ist intern und extern bereits erfolgt, aber keine geeigneten Folgemaßnahmen wurden ergriffen. Weiters erlaubt die Richtlinie die Offenlegung von Meldungen, wenn der Hinweisgeber gem. Art. 8 Abs. 1 WBRL den hinreichenden Grund zur An-

nahme hat, dass eine offenkundige Gefährdung des öffentlichen Interesses existiert, Repressalien befürchtet werden müssen oder die Gefahr der Beweismittelunterdrückung sowie -vernichtung besteht oder die zuständige Behörde am Verstoß selbst beteiligt sein könnte.

IV. Anonyme Meldekanäle

Die Zulassung anonymer Meldungen an Meldestellen wird gem. Art. 6 Abs. 2 WBRL dem nationalen Gesetzgeber überlassen. Einerseits soll damit den Zweifeln gegenüber anonymen Hinweisen entgegengekommen werden, da hier häufig Skepsis bezüglich der Motive sowie ihrer Lauterbarkeit besteht. Andererseits wird die Bereitwilligkeit, Verstöße zu melden, bei künftigen Hinweisgebern auch von der Möglichkeit abhängen, die eigene Identität nicht preiszugeben, sondern anonym zu bleiben.[32]

In der Praxis wird eine gänzliche Anonymität des Hinweisgebers trotzdem oft nicht gegeben sein, weil durch die Meldung und die darin enthaltenen Informationen oftmals ein Rückschluss auf eine Person oder einen einzugrenzenden Personenkreis möglich ist.[33]

V. Konzerninterne Meldekanäle

Für Unternehmensgruppen und Konzerne kann es aus Effizienz- und Kostengründen erstrebenswert sein, ein gemeinsames Whistleblowing-System einzurichten, anstatt jede juristische Person innerhalb des Konzerns mit einem eigenen Meldekanal auszustatten. Grundsätzlich sieht die WBRL auch vor, dass juristische Personen des Privatrechts gemeinsam eine Whistleblowing-Stelle betreiben können. Diese Möglichkeit ist jedoch gem. Art. 8 Abs. 6 WBRL auf Unternehmen mit 50 bis 249 Arbeitnehmern limitiert. Für Konzerne, die in der Mutter- und den Töchtergesellschaften jeweils über 250 Personen beschäftigen, würde dies bedeuten, dass die Konzerne keinen gemeinsamen internen Meldekanal einrichten können. Nach Ansicht der europäischen Kommission genügt ein konzernweites Whistleblowing-System den Anforderungen der WBRL nicht. Dies geht aus zwei Stellungnahmen der Kommission hervor, die den Anfragen von europäischen Großkonzernen folgten. Demnach sei ein zentral im Kon-

32 Schmolke NZG 2020, 5 (9).
33 Artikel 29 Gruppe WP 117, 11.

zern angesiedeltes System contra legem und jede Tochtergesellschaft müsse ein eigenständiges, dezentrales Hinweisgebersystem betreiben. Art. 8 Abs. 6 WBRL wird von der Kommission so ausgelegt, dass auch Tochtergesellschaften die zentrale Meldestelle des Konzerns wählen dürfen, allerdings müssen gleichzeitig eigene Meldekanäle angeboten werden. Zusätzlich muss der Hinweisgeber seine Zustimmung geben, die Ermittlung an der zentralen Stelle erfolgen zu lassen. Verweigert er, die Übertragung der Ermittlung an die konzernzentrale Stelle zu bewilligen, ist der gemeldete Verstoß ausschließlich auf der Ebene der Tochtergesellschaft zu untersuchen. Das Ergebnis dieser Ermittlung darf dann jedoch nach Ansicht der Kommission konzernintern übermittelt werden.

Für Großkonzerne mit Töchtergesellschaften von über 250 Mitarbeitern würde dies zudem bedeuten, dass der Art. 8 Abs. 6 WBRL nicht einschlägig ist und jede Gesellschaft allein für die Einrichtung der Meldekanäle und Ermittlungen zuständig ist.[34]

D. Schutzmaßnahmen

Kapitel VI der WBRL enthält einen Katalog von Maßnahmen zum Schutz der Hinweisgeber und betroffener Personen. Es werden ebenso Sanktionen festgelegt, die auf der einen Seite die Wirksamkeit der Schutzregelungen garantieren sowie andererseits einen abschreckenden Effekt gegen böswillige Meldungen und Repressalien erzielen sollen gem. Erwgr. 102 WBRL.

I. Schutz für Hinweisgeber

Anspruch auf Schutz besitzen in einem ersten Schritt nur jene Hinweisgeber, die vom persönlichen Schutzbereich der Richtlinie umfasst werden. Das Recht auf Schutz eines Hinweisgebers besteht nach Art. 6 Abs. 1 lit. a WBRL weiters nur, wenn der Hinweisgeber hinreichende Gründe zur Annahme hatte, dass der Verstoß in den Anwendungsbereich der WBRL fällt und die Informationen der Zuwiderhandlung zum Zeitpunkt der Meldung der Wahrheit entsprachen.

Für den Schutz des Whistleblowers reicht es aus, dass Letzterer zum Zeitpunkt der Meldung im guten Glauben ist, dass ein Verstoß erfolgt

34 Block/Kremer, Whistleblowing im Konzern: Eine zentrale Stelle ist zu wenig! abrufbar unter: https://www.cmshs-bloggt.de/compliance/whistleblowing-im-konzern-eine-zentrale-stelle-ist-zu-wenig/. (Stand 15.12.2023).

ist. Dieser muss nicht nachweislich vorliegen. Die Richtlinie gibt keine Kriterien für eine Bewertung vor, wann eine Meldung ‚hinreichend' ist. Gemäß Erwägungsgrund 32 ist dies *„eine Schutzvorkehrung gegen böswillige oder missbräuchliche Meldungen, da sie gewährleistet, dass Personen keinen Schutz erhalten, wenn sie zum Zeitpunkt der Meldung willentlich und wissentlich falsche oder irreführende Informationen gemeldet haben."* (Erwgr. 32 S. 3 WBRL)

Wie in Erwgr. 32 S. 5 WBRL festgelegt, sind die subjektiven Motive des Whistleblowers, die ihn zu einer Meldung veranlassen, bei der Frage der Schutzwürdigkeit nicht relevant.

Durch die Voraussetzung der Gutgläubigkeit wird den Whistleblowern der Weg zu einer Meldung oder Offenlegung erleichtert, da es für Laien vermutlich in vielen Fällen schwierig zu erkennen ist, ob der Verstoß nun konkret in den Anwendungsbereich der Richtlinie fällt oder nicht.[35]

Gemäß Art. 6 Abs. 1 lit. b WBRL ist der Schutz des Whistleblowers darüber hinaus an die Voraussetzung geknüpft, dass er intern einen Verstoß meldet oder eine Offenlegung vorgenommen hat. Bei Meldungen, die ein Whistleblower anonym erstattet und bei denen jedoch im Nachhinein seine Identität bekannt wird, erhält er ebenso Schutz vor Repressalien nach Art. 6 Abs. 3 WBRL.

II. Untersagung von Repressalien

Der Begriff der Repressalien wird in Art. 5 Ziff. 11 WBRL legaldefiniert. Darunter zu verstehen sind direkte oder indirekte ungerechtfertigte Handlungen sowie Unterlassungen in einem beruflichen Kontext, die nach einer Meldung oder Offenlegung i. S. d. Richtlinie erfolgen. Für einen umfassenden Schutz des Hinweisgebers ist auch der Begriff der Repressalien äußerst weit gefasst.

Die Mitgliedstaaten müssen nach Art. 19 WBRL jegliche Form von Repressalien, die sich gegen schützenswerte Whistleblower richtet, und deren Androhung verbieten. Beispiele für Repressalien werden außerdem in Art. 19 aufgelistet. Dies können etwa eine Kündigung, Suspendierung, Herabstufung, negative Leistungsbeurteilung oder Mobbing und Diskriminierung sein (Art. 19 WBRL).

35 Kröll/Stumpf RdW 2020, 161 (162).

Den Hinweisgebern sind nach Art. 20 Abs. 2 WBRL unterstützende Maßnahmen anzubieten. Dazu gehört unter anderem eine kostenlose, öffentlich zugängliche Beratung über Abhilfemöglichkeiten und Rechte der betroffenen Person. Die zuständigen Behörden haben außerdem die Hinweisgeber bei der Kommunikation mit anderen Behörden zu unterstützen, die am Schutz vor Repressalien beteiligt sind. Des Weiteren ist eine Prozesskostenhilfe in Strafverfahren für jene Whistleblower bereitzustellen, die sich gerichtlich gegen Repressalien wehren möchten. Ebenso liegt es laut Art. 20 Abs. 2 WBRL in der Hand der Mitgliedstaaten, weitere unterstützende Maßnahmen für Hinweisgeber, wie beispielsweise eine psychologische Beratung, anzubieten, denn in vielen Fällen können die erlittenen Repressalien beim Whistleblower zu finanziellen Schwierigkeiten sowie zu psychischen Auswirkungen führen.[36]

Die Mitgliedstaaten werden nach Art. 21 Abs. 1 WBRL verpflichtet, erforderliche Maßnahmen zu treffen, um die gutgläubig handelnden Hinweisgeber vor Repressalien zu schützen. Die Schutzmaßnahmen gegen Repressalien werden demonstrativ in Art. 21 Abs. 2–8 WBRL gelistet. In Art. 21 Abs. 2 WBRL wird beinahe eine straf- und zivilrechtliche Immunität für Whistleblower festgelegt, demnach können sie für die Verletzung von Berufsgeheimnissen nicht verantwortlich gemacht werden. Noch weitergehender ist der Art. 21 Abs. 7 WBRL: So haben Hinweisgeber in Gerichtsverfahren wegen Verleumdung, Urheberrechts- und Geheimhaltungspflichtverletzungen sowie Verstößen gegen Datenschutzvorschriften, Geschäftsgeheimnisse und Schadensersatzverfahren nicht belangt zu werden. Sie haben zudem die Möglichkeit, eine Klageabweisung zu beantragen.

Nach Art. 21 Abs. 3 WBRL kann ein Hinweisgeber nicht für die Beschaffung der Informationen, die gemeldet werden sollen, belangt werden. Wird beim Erwerb dieser Informationen durch Hinweisgeber jedoch eine Straftat begangen – Erwgr. 92 WBRL nennt hier etwa Hacking oder Hausfriedensbruch –, so greift der Haftbarkeitsausschluss nicht.

Ein weiterer hervorzuhebender Schutzmechanismus ist die in Art. 21 Abs. 5 WBRL geregelte Beweislastumkehr. Legt der Hinweisgeber dar, dass er aufgrund einer getätigten Meldung oder Offenlegung Repressalien erfahren hat, so hat die Partei, die die Repressalien veranlasst hat (zB der Arbeitgeber) entsprechend Art. 21 Abs. 5 WBRL, den Beweis zu erbringen, dass diese auf anderen Gründen als der Meldung basieren.

36 Dilling CZZ 2019, 214 (216).

III. Schutz der betroffenen Person

Neben dem Schutz von Hinweisgebern wird auch jenem der betroffenen Personen in der Richtlinie Rechnung getragen, um eine Rufschädigung und weitere negative Folgen in der Sphäre des Beschuldigten zu vermeiden (Erwgr. 100 WBRL). Demnach müssen die Mitgliedstaaten nach Art. 22 Abs. 1 WBRL sicherstellen, dass die betroffenen Personen gem. der Grundrechte-Charta den Zugang zu wirksamen Rechtsbehelfen, ein faires Verfahren und die Wahrung der Unschuldsvermutung haben. Weiters müssen in einer Meldung beschuldigte Personen ihre Verteidigungsrechte sowie die Rechte auf Anhörung und auf Akteneinsicht vollumfänglich ausüben können. Die Identität der betroffenen Person ist außerdem während der gesamten Dauer einer Meldung durch die zuständigen Behörden und dadurch eingeleitete Folgemaßnahmen zu schützen (Art. 22 Abs. 2 WBRL).

IV. Sanktionen

Gemäß Art. 23 Abs. 1 WBRL wird der Schutz der Hinweisgeber auf der einen Seite noch verstärkt, indem die Richtlinie vorschreibt, dass Mitgliedsstaaten *„wirksame, angemessene und abschreckende Sanktionen"* gegen juristische oder natürliche Personen verhängen, welche Repressalien gegen schutzwürdige Personen ergreifen, Meldungen behindern oder dies versuchen, mutwillig gerichtliche Verfahren anstreben oder gegen den Vertraulichkeitsgrundsatz der Richtlinie in Art. 14 WBRL verstoßen.

Demgegenüber wird in Abs. 2 darüber hinaus festgelegt, dass Hinweisgeber, die wissentlich falsche oder irreführende Informationen gemeldet haben, aus dem Schutzbereich der Richtlinie fallen und dass ihnen **Sanktionen** sowie Schadenersatzpflichten auferlegt werden können.[37] Im Weiteren haben die Mitgliedstaaten entsprechend Art. 23 Abs. 2 WBRL Maßnahmen zur Wiedergutmachung der durch eine Meldung entstandenen Schäden im nationalen Recht umzusetzen.

Zu einem Streitfall können Hinweisgeber werden, die leicht oder grob fahrlässig handeln. In solchen Fällen kann die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zum Kriterium der Authentizität der Informationen herangezogen werden. Demnach hat ein

37 Dilling CZZ 2019, 214 (216).

Whistleblower vor der Meldung sorgfältig zu prüfen, ob die Informationen zum Verstoß zutreffend und ernstzunehmend sind.[38]

§ 4 Umsetzung der Whistleblower-Richtlinie in Unternehmen

Die Implementierung eines Hinweisgebersystems im Unternehmen sollte möglichst so erfolgen, dass die gemeldeten Verstöße effektiv und nach transparenten internen Leitlinien bearbeitet werden können. Damit werden viele Unternehmen vor neue Aufgaben und Schwierigkeiten gestellt – teils, wenn es darum geht, erstmalig Meldekanäle einzurichten, oder wenn bereits bestehende Hinweisgebersysteme auf die neue Rechtslage auszurichten sind. Hinzu kommen bei der Einführung und im Betrieb von Whistleblowing-Systemen datenschutzrechtliche und arbeitsrechtliche Herausforderungen.[39] Das folgende Kapitel widmet sich speziell den daraus resultierenden datenschutzrechtlichen Fragestellungen, im Groben werden auch mit dem Arbeitsrecht in Verbindung stehende Berührungspunkte skizziert.

A. Datenschutzrechtliche Aspekte im Rahmen von Hinweisgebersystemen

Die Datenschutz-Grundverordnung (DSGVO)[40] gilt seit dem 25.5.2018. Als EU-Verordnung ist sie, anders als die WBRL, die erst in nationales Gesetz gegossen werden muss, in allen Mitgliedsstaaten der Europäischen Union unmittelbar anwendbar. Die DSGVO sieht für die Mitgliedsstaaten einige Öffnungsklauseln vor, die durch den nationalen Gesetzgeber ausgestaltet werden können. Diese Möglichkeit hat Österreich mit der Verabschiedung des Datenschutzgesetzes (DSG) teils genutzt. Das DSG ist gleichzeitig mit dem Datenschutzgesetz in Kraft getreten.[41]

Der sachliche Anwendungsbereich der DSGVO ist nach Art. 2 Abs. 1 eröffnet, wenn „*personenbezogene Daten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte*

38 EGMR 16.2.2021, 23922/19.
39 Kröll/Stumpf RdW 2020, 161 (165).
40 VO (EU) 2016/679.
41 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 188.

Verarbeitung personenbezogener Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen."

Unter dem Begriff ‚*personenbezogene Daten*' wird nach Art. 4 Abs. 1 DSGVO die Verarbeitung von Informationen verstanden, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Dabei kann die Verarbeitung der Daten ganz oder teilweise automatisiert oder auch nicht automatisiert vorgenommen werden. So fallen ebenfalls rein manuelle Verarbeitungen in den sachlichen Anwendungsbereich, wenn die Verarbeitung in einer strukturierten Sammlung erfolgt.[42]

Bei einem Hinweisgebersystem wird bei nahezu allen eingehenden Meldungen ein Personenbezug bestehen. Der Inhalt einer Meldung wird jedenfalls den Namen des Beschuldigten und bei einer nicht anonymen Meldung den Namen des Hinweisgebers inkludieren. Darüber hinaus werden meist zusätzliche Informationen mit Personenbezug über den Verstoß enthalten sein, wie die Position im Unternehmen oder weitere Umstände der Beobachtungen des Whistleblowers. In einem weiteren Schritt muss die Meldung auf ihre Plausibilität geprüft werden. Dazu wird es notwendig sein, verschiedene personenbezogene Daten aus Datenbanken oder IT-Systemen auszuwerten. Bei einer Bestätigung des Verdachts werden vermutlich weitere Daten aus E-Mail-Postfächern analysiert. In einem weiteren Schritt wird es auch notwendig sein, abschließend Befragungen durchzuführen, um den Sachverhalt aufzuklären. Bewahrheitet sich die Meldung, so werden die Daten schlussendlich in einem Report an den Vorstand oder die Geschäftsführung übermittelt.

Damit wird eine Vielzahl an personenbezogenen Daten – von der Entgegennahme des Hinweises bis hin zur Übermittlung einer sachverhaltsklärenden Stellungnahme – verarbeitet, während der Anwendungsbereich der DSGVO als eröffnet gilt.[43] Jede Verarbeitung von personenbezogenen Daten stellt aber einen Eingriff in das Grundrecht auf Datenschutz des Einzelnen dar. Bei der DSGVO handelt es sich um ein Verbotsgesetz mit Erlaubnisvorbehalten. Demnach ist eine Verarbeitung von personenbezogenen Daten nur erlaubt, wenn die Verarbeitung auf Grundlage der Grundsätze der DSGVO nach Art. 5 stattfindet und die Datenverarbeitung auf Basis einer legitimen Rechtsgrundlage nach Art. 6 erfolgt.[44]

42 Kühling/Raab/Buchner DS-GVO BDSG (2020) Art. 2 Rn. 19.
43 Fehr ZD 2022, 256.
44 Petsche Whistleblowing & Internal Investigations S. 225.

Vor diesem Hintergrund ist es für Unternehmen in der Praxis entscheidend, die Bestimmungen der DSGVO auch bei der Implementierung und im Betrieb eines internen Meldekanals angemessen zu beachten. Schließlich können Unternehmen aus datenschutzrechtlicher Sicht für alle Handlungen im Rahmen des Hinweisgebersystems verantwortlich gemacht werden sowie in Folge Adressat von Bußgeldern oder Schadenersatzforderungen sein.[45]

B. Die rechtmäßige Verarbeitung personenbezogener Daten nach Artikel 6 DSGVO

Personenbezogene Daten können nach Art. 6 DSGVO nur verarbeitet werden, wenn es hierfür eine datenschutzrechtliche Grundlage gibt. Der Verantwortliche – bei Hinweisgebersystemen also in den meisten Fällen das Unternehmen – ist für dessen Einhaltung zuständig. Bei der Abgabe einer Meldung an eine interne Meldestelle werden personenbezogene Daten verarbeitet. Infolgedessen braucht es eine konkrete Rechtsgrundlage, auf die sich die Einrichtung eines Whistleblowing-Systems stützt. Hierfür muss eine der in Art. 6 Abs. 1 lit. a – f aufgezählten Voraussetzungen vorliegen. In einem weiteren Schritt sollen die Rechtgrundlagen, die Einwilligung (lit. a), die Befolgung eines Vertrages (lit. b), die Erfüllung einer rechtlichen Verpflichtung (lit. c) sowie die berechtigten Interessen des Verantwortlichen (lit. f) näher betrachtet werden.

Die Rechtsgrundlage des lebensnotwendigen Interesses (lit. d) sowie die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (lit. e), können bei der Verarbeitung von personenbezogenen Daten durch das Betreiben eines Hinweisgebersystems wohl ausgeschlossen werden.

I. Die Einwilligung lit. a

Dabei wäre die Einwilligung aller Mitarbeiter des Unternehmens in die Verarbeitung ihrer personenbezogenen Daten durch das Betreiben eines Whistleblowing-Systems der unkomplizierteste Weg. Letzterer ist jedoch aus mehreren Gründen als äußerst kritisch anzusehen. Die Einwilligung muss freiwillig und in informierter sowie unmissverständlicher Weise abgegeben werden. Hier stellt sich die Frage, ob die Einwilligung überhaupt

45 Fehr ZD 2022, 256.

freiwillig erfolgen kann oder ob Mitarbeiter, aufgrund der bestehenden Weisungsgebundenheit und des Abhängigkeitsverhältnisses, das Gefühl haben, sie müssten der Implementierung eines Hinweisgeberschutzsystems zustimmen, da sie sonst beruflich benachteiligt werden könnten. Der Beweis, dass die Einwilligung aus freien Stücken abgegeben wurde, wird für den Verantwortlichen oft schwer zu erbringen sein. Ebenso kann die Einwilligung nicht in informierter Weise erfolgen, sollte eine allgemeine Einwilligungserklärung eingeholt werden. Schließlich ist vor der Abgabe einer Meldung unklar, wer von der Verarbeitung personenbezogener Daten betroffen sein wird. Die Einwilligung kann außerdem nicht pauschal für die Verarbeitung der personenbezogenen Daten im Rahmen des Whistleblowings gegeben werden, der Art. 4 Ziff. 11 DSGVO verlangt nämlich, dass die Einwilligung für den bestimmten Fall erfolgen muss.

Eine Einwilligung für Letzteren kann auch nur vom Hinweisgeber selbst erfolgen und hier nur für die Verarbeitung seiner eigenen personenbezogenen Daten. Er kann nicht in die Verarbeitung der Daten des Beschuldigten oder Dritter einwilligen. Spätestens hier ist die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO gescheitert und damit keine legitime Rechtgrundlage.[46]

II. Die Erfüllung eines Vertrages lit. b

Art. 6 Abs. 1 lit. b DSGVO wird als taugliche Rechtsgrundlage für die Datenverarbeitung bei Whistleblowing-Systemen ebenso ausscheiden, weil diese wohl nicht mehr mit der Erfüllung des Arbeitsvertrages gerechtfertigt werden kann.[47] Die Datenverarbeitung dient schlussendlich nicht den Beschäftigungsverhältnissen an sich, sondern der Durchsetzung von internen Compliance-Interessen.[48]

46 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 194.

47 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

48 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 196.

III. Die Erfüllung einer rechtlichen Verpflichtung lit. c

Bisher konnten sich nur Unternehmen in ausgewählten Branchen wie dem Bankwesen, wo die Pflicht zur Einrichtung von Meldekanälen bereits gesetzlich vorgeschrieben ist, auf die Rechtgrundlage nach Art. 6 Abs. 1 lit. c stützen.[49] Mit der Umsetzung der WBRL wird sich dies jedoch ändern, da alle Unternehmen mit mehr als 49 Mitarbeitern Hinweisgeberkanäle einrichten müssen. Hiervon erfasst sind jedoch nur Meldungen von Verstößen, die ebenfalls in den sachlichen Anwendungsbereich fallen. Werden darüber hinaus weitere Meldungen abgegeben, die Verstöße gegen weitere Gesetze oder die unternehmensinterne Compliance-Richtlinie aufzeigen sollen, sind diese von der Erfüllung einer rechtlichen Verpflichtung nicht abgedeckt. Auch Unternehmen, die nicht dem Anwendungsbereich der WBRL angehören, weil sie etwa weniger als 50 Arbeitnehmer beschäftigten, können sich nicht auf diese Rechtsgrundlage berufen.[50]

IV. Das berechtigte Interesse des Verantwortlichen lit. f

Für alle Meldungen, die nicht von der Erfüllung einer rechtlichen Verpflichtung umfasst werden, müssen Unternehmen den Erlaubnistatbestand gem. Art. 6 Abs. 1 lit. f DSGVO heranziehen. Die Verarbeitung personenbezogener Daten ist demnach nur zulässig, wenn diese zur Wahrung des berechtigten Interesses des Verantwortlichen erforderlich sind und schwerer wiegen als der Schutz der Grundrechte des Betroffenen.[51] In der Praxis wird es daher erforderlich sein, eine Prüfung des berechtigten Interesses vorzunehmen, ob im Einzelfall die Datenverarbeitung notwendig ist, um das angestrebte Ziel zu erreichen. Ein solches berechtigtes Interesse wird zu bejahen sein, wenn es um die Prävention von Strafverfolgungen, Imageschäden oder massiven wirtschaftlichen Schäden geht. Anders zu bewerten ist die Interessenabwägung, wenn sich der Verstoß gegen den Compliance- oder Ethik-Kodex richtet.[52]

49 Fehr ZD 2022, 256 (257).
50 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 197
51 Altenbach/Dierkes CCZ 2020, 126 (127).
52 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 198.

Bei der Etablierung von Meldekanälen in Unternehmen ist daher ein Augenmerk, darauf zu legen, welche Art und Schwere von Verstößen gemeldet werden. Jede Verarbeitung von personenbezogenen Daten durch Verstöße, die nicht in den gesetzlich definierten Anwendungsbereich fallen, muss vom berechtigten Interesse gedeckt sein. Je weitgehender der Inhalt der Meldung in einem Unternehmen ist, desto schwieriger wird es aus datenschutzrechtlicher Sicht für den Verantwortlichen, gegen den Schutz und die Wahrung der Grundrechte des Betroffenen zu argumentieren. Aus diesem Grund sollten die Beschäftigten ebenfalls dazu angehalten werden, lediglich jene Verstöße zu melden, die strafrechtlich relevant sind, und keine Banalitäten, die voraussichtlich auch von internen Meldestellen nicht verfolgt werden.[53]

Für kleine Unternehmen wurde hier keine Abhilfe geschaffen. Sie stehen vor der gleichen Situation wie vor der Umsetzung der WBRL und können sich derzeit nur auf das berechtigte Interesse stützen.

Eine mögliche Alternative wäre es jedoch, sich auf Art. 88 DSGVO zu berufen. Dieser sieht vor, dass der nationale Gesetzgeber anhand von *„Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext"* festlegen kann. Da es sich bei Art. 88 DSGVO allerdings um eine Öffnungsklausel handelt, haben nicht alle Mitgliedstaaten diese Möglichkeit genutzt. Dies gilt auch für den österreichischen Gesetzgeber[54], weshalb der datenschutzrechtliche Aspekt von Whistleblowing-Systemen für österreichische Unternehmen auf Grund fehlender spezifischerer Vorschriften im Beschäftigungskontext gesetzlich nicht vorgesehen ist und die Möglichkeit der Kollektivvereinbarung, anders als etwa in Deutschland[55], damit keinen gangbaren Weg darstellt.

Arbeitsverfassungsrechtliche Aspekte zur Umsetzung von internen Hinweisgebersystemen in Unternehmen werden im Folgenden in Kap. 4 skizziert.

53 Schmidl in Hauschka/Moosmayer/Lösler Corporate Compliance § 28 Rn. 340.

54 Brodil ecolex 2018, 486 (488).

55 Datenschutzkonferenz Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf. (Stand 15.12.2023).

V. Verarbeitung von personenbezogenen Daten nach Artikel 10 DSGVO

Basiert die Verarbeitung von personenbezogenen Daten auf einer tauglichen Grundlage nach Art. 6 DSGVO, muss geprüft werden, ob auch Daten nach Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten verarbeitet werden. Art. 10 DSGVO wird in Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch Hinweisgebersysteme, je nach Art und Schwere des gemeldeten Verstoßes, eine Rolle spielen. Die Verarbeitung der Daten ist demnach unter behördlicher Aufsicht erlaubt oder *„wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten [gestattet ist], das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.* (Art. 10 DSGVO)

Wird davon ausgegangen, dass auch der Verdacht auf eine begangene Straftat von der Bestimmung des Art. 10 umfasst wird, so ist es für Unternehmen nur dann zulässig, ein Whistleblowing-System einzurichten, wenn sie nach dem nationalen Recht oder dem Unionsrecht der gesetzlichen Pflicht dazu unterliegen. Laut dem DSG ist gem. § 4 Abs. 3 Ziff. 2 ebenfalls die Verarbeitung von personenbezogenen Daten über gerichtliche oder verwaltungsbehördlich strafbare Handlungen und über den Verdacht der Begehung einer Straftat unter Einhaltung der DSGVO gestattet, sofern sich die Zulässigkeit der Datenverarbeitung aus gesetzlichen Sorgfaltspflichten ergibt oder diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten laut Art. 6 Abs. 1 lit. f DSGVO erforderlich ist. Hierbei müssen bei der Art der Verarbeitung der Daten die Interessen des Betroffenen nach der DSGVO und dem DSG garantiert werden. Daraus ist zu schließen, dass das berechtigte Interesse eines Unternehmens gleichsam als Rechtsgrundlage für die Verarbeitung von Daten nach Art. 10 DSGVO herangezogen werden kann.[56]

C. Die datenschutzrechtliche Rollenverteilung

Die DSGVO richtet sich an differente Akteure, die auf Grund ihrer Verpflichtungen zu unterscheiden sind. Die Klärung dieser Rollenverteilung ist daher eine grundlegende Frage im Datenschutzrecht, weil von dieser Frage wesentliche Rechts- und Haftungsfragen abhängig gemacht werden.

56 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 200.

Das Ziel der verschiedenen Rollen liegt darin, dass auch beim Zusammenwirken mehrerer Akteure und komplexer Strukturen die Wahrung des Datenschutzes und damit der Schutz personenbezogener Daten garantiert werden können.[57]

In der Praxis müssen sich Unternehmer bei Einführung eines Hinweisgebersystems entscheiden, ob dies ein innerhalb des Unternehmens geführtes Meldesystem ist oder ob dieses an eine externe, nicht direkt im Unternehmen angesiedelte Person oder Organisation ausgelagert wird. Dies kann etwa ein Call-Center oder eine plattformbasierte Whistleblowing-Stelle sein. Daraus ergibt sich in weiterer Folge auch die Rollenverteilung. Ebenso ist für Unternehmensgruppen und Konzerne zu prüfen, inwieweit die datenschutzrechtliche Möglichkeit besteht, für alle juristischen Personen gemeinsam ein Hinweisgebersystem zu betreiben.

I. Die Auftragsverarbeitung nach Artikel 28 DSGVO

Bei einem intern geführten Meldesystem ist der Unternehmer demnach gem. Art. 4 Ziff. 7 DSGVO der Verantwortliche. Letzterer trägt die Entscheidungsfunktion und bestimmt damit über Mittel und Zweck der Verarbeitung personenbezogener Daten. Damit ist er sowohl für die Mehrheit der Pflichten nach der DSGVO als auch für das wesentliche Haftungsobjekt verantwortlich.

Fällt die Wahl auf ein ausgelagertes Hinweisgebersystem, werden durch die Meldung personenbezogener Daten des Hinweisgebers, der betroffenen Person und Dritten wie Zeugen durch einen externen Empfänger verarbeitet. In diesem Fall muss geklärt werden, ob der externe Dritte in einem Auftragsverarbeitungsverhältnis zum Verantwortlichen steht oder ob dieser selbst die Rolle des Verantwortlichen innehat.

Wird der externe Empfänger damit beauftragt, die Meldung zu empfangen, aufzuarbeiten und die Informationen an eine vom Unternehmen benannte Person weiterzuleiten, die dann über Folgemaßnahmen zu entscheiden hat, so wird er klar als Auftragsverarbeiter anzusehen sein. Dementsprechend muss nach Art. 28 DSGVO ein Auftragsverarbeitungsvertrag abgeschlossen werden, wodurch der Datentransfer legitimiert wird und keine zusätzliche Rechtsgrundlage nötig ist. Der Rolle des Auftragsverarbeiters liegt zu Grunde, dass dieser die Verarbeitung ausschließlich auf Weisung des Verantwortlichen vornehmen darf.

57 Artikel-29-Datenschutzgruppe WP 117, 1.

Eine andere Verteilung der Rollen ist gegeben, wenn der Betreiber des externen Meldesystems auch mit der eigenständigen Entscheidung über Folgemaßnahmen, die Ermittlungen und die Nachforschung der Meldung oder der Befragung beauftragt wird. Auf Grund der mangelnden Weisungs- sowie Kontrollmöglichkeiten des Unternehmers gegenüber dem externen Empfänger liegt dann kein Auftragsverarbeitungsverhältnis vor. Der Externe wird in dieser Konstellation zu einem Verantwortlichen. Dies wiederum bedeutet, dass die Datenübermittlung nicht durch einen Auftragsverarbeitungsvertrag legitimiert werden kann, sondern die Datenübermittlung auf einer eigenen Rechtsgrundlage beruhen muss.

Hier kommen einerseits der Art. 6 Abs. 1 lit. c DSGVO und damit die Erfüllung einer gesetzlichen Pflicht zum Tragen. Da aber der externe Empfänger nicht gesetzlich dazu verpflichtet ist, ein Whistleblowing-System für ein fremdes Unternehmen zu betreiben, ist fraglich, ob der lit. c überhaupt eine geeignete Grundlage darstellt. In diesem Fall wird auf Grundlage des Vertrages zwischen dem Unternehmen und der Whistleblowing-Stelle wohl die Rechtsgrundlage der Erfüllung einer vertraglichen Verpflichtung nach lit. b zum Tragen kommen. Andererseits wird die Rechtsgrundlage des berechtigten Interesses des Unternehmens im Sinne des Art. 6 Abs. 1 lit. f in Betracht gezogen werden können.[58]

Sollte zudem ein Unternehmen mit Sitz im Europäischen Wirtschaftsraum (EWR) einen externen Dritten außerhalb des EWR mit der Entgegennahme der Meldungen beauftragen, so muss geprüft werden, ob es sich hierbei um ein ‚sicheres Drittland' handelt. Dies ist der Fall, wenn nach Art. 45 DSGVO ein Angemessenheitsbeschluss der Europäischen Kommission existiert. Liegt ein solcher nicht vor, handelt es sich um ein sogenanntes ‚unsicheres Drittland' und es müssen geeignete Garantien nach Art. 46 DSGVO getroffen werden. Dies kann der Abschluss der Standardvertragsklauseln der Europäischen Kommission oder von Binding Corporate Rules gem. Art. 47 DSGVO sein.[59]

58 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 204.

59 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 206.

II. Die Gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO

Unter dem Aspekt der datenschutzrechtlichen Rollenverteilung muss auch ein Blick auf die Datenübermittlung durch Whistleblowing-Systeme innerhalb eines Konzerns geworfen werden. Schließlich sieht die DSGVO kein Konzernprivileg bei der Übermittlung von Daten vor. Verbundunternehmen sind untereinander wie Dritte iSd. Art. 4 Ziff. 10 zu sehen. Deshalb bedarf die Datenübermittlung zwischen konzernverbundenen Unternehmen einer tauglichen Rechtgrundlage, anzudenken ist hier das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO.[60]

So könnte ein berechtigtes Interesse des Mutterunternehmens an gemeldeten Verstößen in den Konzerntöchtern argumentiert werden. Die Weiterleitung von ausnahmslos allen gemeldeten Verstößen in einem konzernangehörigen Unternehmen kann sich jedoch nicht auf berechtigte Interessen stützen. Hier sollte der Fokus auf jene Meldungen gelegt werden, die Personen beschuldigen, die durch ihre Funktion eine weitreichende Einflussnahme im Unternehmen haben. Alternativ sollte der Schwerpunkt auf Mitarbeiter gelegt werden, denen zwar nur ein geringer Einfluss innerhalb des Konzerns zukommt, deren Verstoß aber derart schwerwiegend ist, dass ein überwiegendes berechtigtes Interesse der Konzernmutter an der Datenübermittlung besteht. Der Erlaubnistatbestand des Art. 6 Abs.1 lit. f DSGVO wird damit nicht pauschal als Grundlage dienen können, sondern erfordert im Einzelfall eine Interessenabwägung zwischen dem Interesse des Verantwortlichen und den Rechten und Freiheiten der Betroffenen.[61]

Eine weitere Möglichkeit, die bei der Datenübermittlung innerhalb eines Konzernes vorliegen kann, ist die gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO. Dies wäre der Fall, wenn mehrere Unternehmen eines Konzerns gemeinsam einen Meldekanal betreiben. Hierfür müsste eine Vereinbarung über die gemeinsame Verantwortlichkeit geschlossen werden.[62]

Nach Meinung der Art.-29-Datenschutzgruppe soll die Bearbeitung von Hinweisen grundsätzlich von dem Unternehmen des Mitgliedsstaates vorgenommen werden, in dem die Meldung erfolgte. Umfasst ein Konzern

60 Moos/Schefzig/Arning Praxishandbuch DSGVO 56.
61 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 207.
62 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 205

Gesellschaften in verschiedenen EU-Ländern, so sollen die Hinweise nicht automatisch an die Unternehmensgruppe weitergeleitet werden. Hiervon kann eine Ausnahme erfolgen, wenn die Art oder die Schwere des Verstoßes oder auch die Konzernstruktur eine Weiterleitung erforderlich machen.[63]

Sollte bei einem länderübergreifenden Konzern die Übermittlung von Hinweisen ebenfalls in Ländern außerhalb des EWR und damit in ein Drittland erfolgen, so ist wiederum zu beachten, dass die Bestimmung des Kapitels V der DSGVO zur Übermittlung personenbezogener Daten an Drittländer zu erfüllen ist.[64]

D. Spannungsfeld Hinweisgeberschutz und Betroffenenrechte

Bei gemeldeten Verstößen durch Whistleblowing-Systeme ist meist nur ein kleiner Personenkreis unmittelbar für deren Überprüfung und Aufklärung zuständig, um die Verdunklungsgefahr und das Vernichten von Beweisen zu verhindern. Demgegenüber stehen nun die Aufklärungs- und Unterrichtungspflichten nach der DSGVO, die die Aufklärung des Verstoßes und den Schutz des Hinweisgebers gefährden können. Anhand des folgenden Beispiels soll das Spannungsverhältnis zwischen der WBRL und der DSGVO kurz angerissen werden.

Der Verantwortliche hat nach Art. 13 und 14 DSGVO gegenüber Betroffenen seine Informationspflichten zu erfüllen und muss diese darüber in Kenntnis setzen, wenn er deren personenbezogene Daten verarbeitet. Demnach muss eine Person auch darüber informiert werden, wenn sie in einer Meldung beschuldigt wird, ein Fehlverhalten gesetzt zu haben. Zusätzlich stehen den Betroffenen – also den Beschuldigten – ebenfalls die Betroffenenrechte nach Kapitel IIIDSGVO offen. Bekommt diese Person nun Kenntnis von den Ermittlungen gegen sie, so kann diese nach Art. 15 DSGVO bei der Meldestelle eine Kopie der Daten verlangen, die Gegenstand der Ermittlungen sind. Somit könnte der Beschuldigte versuchen, sich gegen die Vorwürfe zu wehren oder Beweise zu vernichten, womit die Aufklärung des Verstoßes gefährdet wäre.[65]

63 Artikel 29 Gruppe WP 117, 18
64 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 192
65 Fehr ZD 2022, 256 (259).

Weiters kann der Beschuldigte auch die Löschung dieser Daten verlangen oder behaupten, die verarbeiteten Daten seien unrichtig, und diese berichtigen lassen.

Nachfolgend soll aufgezeigt werden, wie ein solches Spannungsverhältnis in der Praxis aufgelöst werden könnte.

I. Informationspflicht nach Artikel 13 und 14 DSGVO im Verhältnis zum Hinweisgeberschutz

Der Hinweisgeber selbst kann bei der Abgabe seiner Meldung über die Verarbeitung gem. Art. 13 DSGVO unterrichtet werden. Eine Ausnahme besteht bei der Einreichung einer anonymen Meldung, da in diesem Fall keine personenbezogenen Daten des Betroffenen verarbeitet werden. Sollte im Zuge der Übermittlungen oder durch die abgegebenen Informationen in der Hinweismeldung die Identität des Whistleblowers bekannt werden, so ist die Informationspflicht nach Art.13 zu wahren und der Hinweisgeber über die Verarbeitung zu informieren.[66]

Bei fast allen gemeldeten Verstößen wird der Beschuldigte in der Regel aber nicht wissen, dass seine personenbezogenen Daten durch die Abgabe des Hinweises verarbeitet werden und ihm vom Hinweisgeber ein Vergehen vorgeworfen wird.

Werden die Daten nicht direkt bei den Betroffenen selbst erhoben, so muss nach Art. 14 DSGVO über sämtliche Umstände wie die Speicherung der Daten, die Art dieser Daten, Zwecke der Datenverarbeitung, den Namen und die Kontaktdaten des Verantwortlichen innerhalb eines Monats ab Erhebung der Daten informiert werden. Dies gilt ebenso für Betroffene, die in einer Hinweisgebermeldung eines Verstoßes beschuldigt werden. Im Sinne der Aufklärung von Verstößen und dem Hinweisgeberschutz ist es jedoch kontraproduktiv, den Beschuldigten gem. Art. 14 DSGVO zu unterrichten, weil dies eine Verdunklungsgefahr birgt und der Beschuldigte Beweise vernichten könnte. Diesem Umstand kann mit der Ausnahmebestimmung des Art. 14 Abs. 5 lit. b DSGVO entgegengewirkt werden. Demnach kann die Informationserteilung aufgeschoben werden, wenn dadurch die Verwirklichung der Ziele der Verarbeitung unmöglich gemacht oder ernsthaft beeinträchtigt wird. Diese Ausnahme ist jedoch nicht dauerhaft.

66 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 208.

Sobald der Grund für die Aufschiebung wegfällt, muss die Unterrichtung des Betroffenen unverzüglich nachgeholt werden. Dies wäre der Fall, sobald alle notwendigen Informationen zur Überprüfung des gemeldeten Verstoßes zusammengetragen worden sind. Aus der Sicht der Verantwortlichen besteht ein Risiko, die Erforderlichkeit für die Legitimation des Ausnahmetatbestandes nicht richtig einzuschätzen und den Betroffenen zu spät über die Verarbeitung seiner personenbezogenen Daten zu informieren. Eine Verletzung der Informationspflicht kann für das Unternehmen nach Art. 83 Abs. 5 lit. b DSGVO auch zu einem Bußgeld von bis zu 20.000.000 EUR oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs führen.[67]

Auf der Seite des Hinweisgebers erscheint es zudem problematisch, dass laut Art. 14 Abs. 2 lit. f DSGVO ebenfalls die Quelle offenzulegen ist, aus der die personenbezogenen Daten stammen. Das heißt, sofern die Meldung nicht anonym abgegeben wurde, muss die Identität des Whistleblowers offengelegt werden. Die Preisgabe der Identität eines Hinweisgebers nach der DSGVO steht jedoch in einem eindeutigen Widerspruch zum Schutz des Hinweisgebers nach der WBRL. Nach Ansicht der Art.-29-Datenschutzgruppe[68] ist, sofern dies nicht unmöglich ist, die genaue Datenquelle anzugeben. Die Unmöglichkeit nimmt dabei Bezug auf die Rückführbarkeit der personenbezogenen Daten auf die Datenquelle. Bei einer nicht namentlichen Offenlegung der Quelle muss dem Betroffenen jedoch die Art der Quelle genannt werden. Die Art.-29-Datenschutzgruppe vertritt hier die Ansicht, dass in diesem Fall eine rein kategorische Bezeichnung, wie Arbeitnehmer oder Auftragnehmer, ausreicht, um dem Art. 14 Abs. 2 lit. f nachzukommen. Damit ist aber kein völliger Ausschluss der Identifizierbarkeit des Hinweisgebers garantiert. Auch mit der Nennung einer Personenkategorie können Rückschlüsse auf konkrete Personen als Whistleblower gezogen werden, womit der vollumfängliche Schutz von Hinweisgebern nicht gegeben ist.[69]

Diese Pattsituation kann jedoch nach Art. 14 Abs. 5 lit. c DSGVO umgangen werden, wenn durch Rechtsvorschriften der Union oder der jeweiligen Mitgliedstaaten die Erlangung oder Offenlegung ausdrücklich geregelt ist und zudem Maßnahmen zum Schutz der berechtigten Interessen des Be-

67 Altenbach/Dierkes CCZ 2020, 126 (129).
68 Artikel-29-Datenschutzgruppe WP 260 rev.01, 51.
69 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).

troffenen festgehalten werden.[70] Der Art. 23 Abs. 1 lit. i DSGVO gibt den nationalen Gesetzgeber hier in Form einer Öffnungsklausel Handlungsspielraum, wonach die Informationspflicht im Rahmen einer Interessensabwägung beschränkt werden kann, um Rechte und Freiheiten anderer Personen zu schützen.

In Deutschland wurde eine solche Regelung, die die Geheimhaltung der Identität des Hinweisgebers schützt, im § 29 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) verankert. Eine Pflicht zur Unterrichtung liegt demnach nicht vor, wenn durch die Information nach Art. 14 DSGVO Auskünfte offenbart würden, die auf Grund des überwiegenden berechtigten Interesses eines Dritten, wie eines Hinweisgebers, geheim gehalten werden müssen. Eine ähnliche Bestimmung wurde durch den österreichischen Gesetzgeber jedoch nicht vorgesehen. Dies würde bedeuten: Sobald die Ausnahmebestimmung zur Informationspflicht wegfällt, müssen diese nachgeholt und der Beschuldigte über die Identität des Hinweisgebers unterrichtet werden.[71]

Wenn die Meldung daher nicht anonym, sondern unter Offenlegung des Namens des Hinweisgebers erfolgt, sollte dieser beim ersten Kontakt des Systems darauf hingewiesen werden, dass seine Identität zwar geschützt wird, der Beschuldigte aber grundsätzlich einen Monat nach der Meldung bzw. sobald die Voraussetzungen für das Aufschieben der Informationspflicht weggefallen sind, informiert werden muss und damit auch die Identität des Hinweisgebers preisgegeben wird. Sollte Letzterer die Meldung trotz dieser Information nicht anonym abgeben, kommt nach Art. 7 Abs. 2 DSGVO die Einwilligung der Person in Frage und es hat die Information über den Widerruf der Einwilligung zu erfolgen. Ein solcher Widerruf wird jedoch nur bis zu einem Monat nach der getätigten Meldung wirksam sein.[72]

II. Die Auskunftspflicht nach Artikel 15 DSGVO im Verhältnis zum Hinweisgeberschutz

Gemäß Art. 15 DSGVO hat ein Betroffener das Recht, eine Bestätigung vom Verantwortlichen zu erhalten, ob und welche personenbezogenen Daten von ihm verarbeitet werden. Der Betroffene hat laut Erwgr. 52

70 Altenbach/Dierkes CCZ 2020, 126 (130).
71 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).
72 Fassbach/Hülsberg GWR 2020, 255 (257).

DSGVO Anspruch auf eine Kopie seiner personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Darüber hinaus muss es der betroffenen Person möglich sein, das Recht auf Auskunft in angemessenen Abständen auszuüben. Der Verantwortliche muss den Betroffenen ebenfalls über die Datenerhebung in Kenntnis setzen. Bei einer indirekten Datenerhebung, wenn die personenbezogenen Daten nicht bei der betroffenen Person selbst gesammelt werden, wie dies bei Hinweisgebersystemen der Fall ist, stellt sich nun wieder die Frage der Offenlegung der Identität des Whistleblowers. Schließlich hat nach Art. 15 DSGVO auch die beschuldigte Person ein Recht auf Auskunft bezüglich der über sie gespeicherten Daten und deren Herkunft.

Art. 15 Abs. 4 sieht hier eine Ausnahmeregelung vor. Das Recht auf Datenkopie kann demnach beschränkt werden, wenn die Rechte und Freiheiten anderer Personen dadurch beeinträchtigt werden. Nach dem Wortlaut des Art. 15 gilt dieser Ausnahmetatbestand zum Schutz der Rechte und Freiheiten anderer Personen, sofern eine Kopie der Daten nach Abs. 3 angefragt wird.

Nachdem mit dem Recht auf Erhalt einer Kopie auch die nach Abs. 1 zu erteilende Auskunft der Verarbeitung personenbezogener Daten gemeint ist, wird damit die Möglichkeit einer Interessensabwägung für das Recht auf Auskunft eröffnet.[73]

Eine pauschale Verweigerung der Auskunft an den Beschuldigten wird durch diese Ausnahme jedoch nicht gerechtfertigt werden können. Im Einzelfall muss das Interesse des Beschuldigten am Auskunftsanspruch gegen das betriebliche Interesse des Verantwortlichen an der Auskunftsverweigerung und gegen das berechtigte Interesse von Dritten, wie dem Hinweisgeber, dessen Identität tunlichst zu schützen ist, abgewogen werden.

Mit dieser Frage beschäftigte sich das deutsche Landesarbeitsgericht (LAG) Baden-Württemberg[74] im Jahr 2018. Im angesprochenen Fall handelte es sich um die erste Entscheidung im deutschsprachigen Raum, die sich mit Auskunftsverlangen in Bezug auf Hinweisgebersysteme befasste. Konkret ging es um eine interne Whistleblowing-Meldung, deren Ermittlung bereits abgeschlossen war, weshalb eine Verdunklungsgefahr oder Beeinträchtigung des Ermittlungserfolgs ausgeschlossen werden konnte.

Für die datenschutzrechtliche Interessensabwägung kam das LAG zur folgenden Erwägung: Die Geheimhaltung einer Informationsquelle kann

73 Paal/Pauly/Paal DS-GVO Art. 15 Rn. 40-43.
74 LAG Baden-Württemberg 17 Sa 11/18.

ein legitimes Interesse darstellen, wenn der Arbeitgeber als Verantwortlicher dem Whistleblower zum Zwecke der internen Aufklärung des gemeldeten Fehlverhaltens Anonymität zusichert. Nach Ansicht des LAG bestehen jedoch auch Fälle, in denen das Geheimhaltungsinteresse hinter das Auskunftsinteresse tritt, etwa wenn der Hinweisgeber eine Meldung wider besseres Wissen abgibt oder leichtfertig unrichtige Informationen weitergibt. In einer solchen Konstellation dürfte das Auskunftsverlangen der beschuldigten Person unter Berücksichtigung eines erhöhten Schutzbedarfes schwerer wiegen.

Die Zusage der Anonymität des Hinweisgebers kann aber nicht schlichtweg als Grund für eine zulässige Auskunftsversagung herangezogen werden. Besteht keine gesetzlich verankerte Geheimhaltungspflicht, sondern wurde diese lediglich vereinbart, ist im Einzelfall eine Interessensabwägung vorzunehmen.

Das LAG verurteilte den Arbeitgeber in seiner Entscheidung dazu, dem beschuldigten Mitarbeiter *„eine Kopie seiner personenbezogenen Leistungs- und Verhaltensdaten, die Gegenstand der vorgenommenen Verarbeitung sind, bereitzustellen"*.[75]

In Deutschland besteht nach § 29 Abs. 1 BDSG, wie bereits beschrieben wurde, keine Auskunftsverpflichtung, sofern dadurch Informationen offengelegt werden, die wegen des überwiegenden berechtigten Interesses eines Dritten geheim zu halten sind. In Österreich kann jedoch auf eine vergleichbare Norm nicht zurückgegriffen werden. Unter Beachtung des Art. 15 Abs. 4 DSGVO sind jedoch auch in Österreich im Einzelfall eine Interessensabwägung vorzunehmen und damit die Vertraulichkeit der Identität des Hinweisgebers sicherzustellen.[76]

Für Unternehmen, die der WBRL unterliegen, schafft hier Art. 16 WBRL Abhilfe und statuiert das Vertraulichkeitsgebot für die Identität des Whistleblowers sowie von Dritten. Unbefugte dürfen keinesfalls Zugang zu den Daten der Meldungen haben. Anzumerken ist jedoch, dass damit nicht alle Dokumente und Unterlagen des Meldekanals umfasst werden, sondern nur jene, aus denen indirekt oder direkte die Identität des Hinweisgebers hervorgeht.[77] Eine Ausnahme bildet der Abs. 2, sofern es sich um eine nach dem nationalen Recht oder dem Unionsrecht *„notwendige und verhältnismäßige Pflicht im Rahmen der Untersuchungen durch nationale Be-*

75 Altenbach/Dierkes CCZ 2020, 126 (129).
76 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).
77 Altenbach/Dierkes CCZ 2020, 126 (129).

hörden oder von Gerichtsverfahren" handelt. Trifft dies zu, darf die Identität des Hinweisgebers offengelegt werden. Davor muss Letzterer jedoch nach Art. 16 Abs. 3 WBRL darüber informiert werden. Auch ist ihm dazu eine schriftliche Begründung zu übermitteln.

Mit dem Spannungsfeld zwischen dem Schutz der Identität des Whistleblowers und der Einhaltung des Datenschutzrechtes beschäftigen sich ebenso die Erwägungsgründe 84 und 85 der WBRL. Die Mitgliedstaaten sollen demnach, um die Wirksamkeit der WBRL zu gewährleisten, die DSGVO und die Rechte der Betroffenen mit gesetzgeberischen Maßnahmen einschränken, soweit und solange dies notwendig ist (Erwgr. 84-85 WBRL). Damit wird es auf die Ausgestaltung der Umsetzungsakte der Mitgliedstaaten ankommen, die DSGVO einzuschränken, um den Schutz von Hinweisgebern zu gewährleisten.

III. Recht auf Berichtigung nach Artikel 16 DSGVO

Art. 16 DSGVO regelt das Recht auf Berichtigung durch den Betroffenen. Demnach hat Letzterer das Recht, vom Verantwortlichen eine unverzügliche Berichtigung seiner inkorrekten personenbezogenen Daten sowie eine Komplettierung von unvollständigen personenbezogenen Daten zu verlangen.[78] Im Zusammenhang mit Hinweisgebersystemen kann dies von Relevanz sein, wenn der Betroffene von der Meldung erfährt, in der er beschuldigt wird, und die Informationen zu seinen personenbezogenen Daten inhaltlich unwahr sind oder der Beschuldigte behauptet, dass diese inkorrekt sind. Für die ermittelnde Meldestelle wird zu diesem Zeitpunkt oft noch nicht klar sein, ob es sich tatsächlich um eine falsche Meldung handelt oder der Betroffene dies nur angibt. Die Berichtigung hat nach Art. 16 S. 1 jedoch unverzüglich zu erfolgen.

Gemäß S. 2 besteht für den Betroffenen zudem die Möglichkeit, die Ergänzung seiner unvollständigen Daten zu verlangen. Personenbezogene Daten gelten als fragmentarisch, wenn diese in Bezug auf die konkrete Verarbeitung so lückenhaft sind, dass der mit der Verarbeitung verfolgte Zweck nicht (mehr) erreicht wird.[79]

Dies wäre der Fall, wenn der Betroffene behauptet, dass die in der Meldung offengelegten personenbezogenen Daten so unvollständig seien,

78 Paal/Pauly/Paal DS-GVO Art. 16 Rn. 13-14.
79 Paal/Pauly/Paal DS-GVO Art. 16 Rn. 18.

dass eine sachverhaltsaufklärende Überprüfung des Verstoßes nicht erzielt werden kann.

Eine derartige Anwendung des Art. 16 DSGVO würde aber gegen den Zweck der WBRL sprechen. Dem Beschuldigten sollte im Sinne der Aufklärung des Verstoßes und der Reduktion der Verdunklungsgefahr nicht schon in einem frühen Stadium der Ermittlungen die Möglichkeit gegeben werden, seine Perspektive darzulegen.

Das Verwaltungsgericht Köln entschied zum Berichtigungsanspruch nach Art. 16 DSGVO, dass es sich bei dem Tatbestandsmal der ‚Unrichtigkeit' nach der unionsrechtlichen Auslegung um ein objektives Kriterium handelt und dieses nur auf Tatsachenangaben anwendbar ist. Demnach kann sich ein Berichtigungsanspruch aus Art. 16 DSGVO nur dann ergeben, wenn feststeht, dass die Daten, die der Verantwortliche verarbeitet, objektiv nicht mit der Realität übereinstimmen, und gleichzeitig sicher ist, dass die vom Betroffenen als richtig erklärten Daten auch tatsächlich mit der Wirklichkeit übereinstimmen.[80]

Eine dahingehende Gewissheit in Zusammenhang mit einem Verlangen auf Berechtigung bei Whistleblowing-Meldungen wird bei der verantwortlichen Meldestelle wohl nicht vorliegen können, weshalb die gespeicherten Informationen eines Hinweises demnach nicht unverzüglich berichtigt werden müssen.

IV. Widerspruchsrecht nach Artikel 21 DSGVO

Art. 21 DSGVO schützt den Betroffenen gegen eine Verarbeitung, die nicht in seinem Willen ist. Nach Abs. 1 kann sich der Betroffene mit dem Widerspruchsrecht jedoch nur gegen eine Verarbeitung wehren, die zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt nach Art. 6 Abs. 2 lit. e DSGVO erforderlich ist oder zur Wahrung des berechtigen Interesses des Verantwortlichen dient, soweit das Interesse des Berechtigten gegenüber der Grundfreiheit des Betroffenen gem. Art. 6 Abs. 1 lit. f DSGVO überwiegt. Die Beschränkung auf die Rechtsgrundlage ergibt sich daraus, dass dem Betroffenen bei der Einwilligung nach lit. a ohnedies die Möglichkeit des jederzeitigen Widerrufs offensteht. Bei Erfüllung eines Vertrages nach lit. b würde der Widerruf wohl einen Vertragsbruch darstellen. Im Falle der Verarbeitung gestützt auf die

80 VG Köln 25 K 2138/19.

Rechtsgrundlage des Art. 6 Abs. 1 lit. c geht das Widerspruchsrecht ebenso vor wie das lebenswichtige Interesse nach lit. d.[81]

Besteht die gesetzliche Verpflichtung zur Führung eines Hinweisgebersystems, so wird der Widerspruch nach Art. 21 DSGVO demnach nicht von praktischer Relevanz sein. Wird der interne Meldekanal freiwillig betrieben und wird hierfür die Rechtsgrundlage nach dem berechtigten Interesse des Verantwortlichen gem. Art. 6 Abs. 1 lit. f herangezogen, ist es im Einzelfall die Aufgabe des Verantwortlichen, eine umfassende Interessenabwägung durchzuführen. Dabei ist das besondere Interesse des Betroffenen gegen das eigene zwingend schutzwürdige Interesse des Verantwortlichen oder einer anderen dritten Person abzuwiegen. Bei einer Datenverarbeitung nach lit. f wird dies schon daraus resultierten, dass sowohl das Interesse des Verantwortlichen als auch des Dritten die Verarbeitung der personenbezogenen Daten des Betroffenen legitimieren. Als schutzwürdig sind hierbei alle Gründe zu sehen, die vom Unionsrecht oder von nationalen Gesetzen anerkannt sind. Der Widerspruch des Betroffenen kann durch den Verantwortlichen damit rechtmäßig verweigert werden, wenn er beweisen kann, dass die Datenverarbeitung auf Grund von zwingendem schutzwürdigem Interesse des Verantwortlichen oder eines Dritten gegenüber den Grundrechten und Freiheiten des Betroffenen überwiegt.[82]

E. Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn die Verarbeitung der personenbezogenen Daten aufgrund der Art, des Umfanges, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen zur Folge hat. Diese Voraussetzungen sind bei einem Hinweisgebersystem zu bejahen, da mit der Meldung Informationen von potenziellen Gesetzesverstößen verarbeitet werden. Dies kann mit zum Teil schwerwiegenden Folgen für den Beschuldigten, den Hinweisgeber und die in der Meldung genannten dritten Personen einhergehen. Damit existiert ein hohes Risiko für die Rechte und Freiheiten der Betroffenen.[83] Dass ein Hinweisgebersystem dem

81 Knyrim/Haidinger DatKomm Art. 21 Rn. 27.
82 Knyrim/Haidinger DatKomm Art. 21 Rn. 42.
83 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendaten-

Art. 35 DSGVO unterliegt, zeigt auch eine Entscheidung der italienischen Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP). Gegen die Flughafenbetreibergesellschaft Aeroporto Guglielmo Marconi di Bologna S.p.A. sowie den externen Betreiber des Whistleblowing-Systems wurde wegen einer fehlenden Datenschutzfolgeabschätzung für den Meldekanal und -prozess für beide insgesamt Parteien eine Geldbuße iHv 60.000 Euro verhängt.[84]

Eine Ausnahme besteht nach der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V). Dieses sieht gem. § 2 Abs. 2 letzter Satz vor, dass eine Datenschutz-Folgenabschätzung nicht zu realisieren ist, wenn die Verarbeitung im Zusammenhang mit dem Arbeitsverhältnis erfolgt und bereits eine Betriebsvereinbarung abgeschlossen wurde. Besteht jedoch kein Betriebsrat, ist es demnach erforderlich, eine Datenschutz-Folgenabschätzung durchzuführen, da die Daten von Arbeitnehmern und damit besonders schutzwürdigen Personen nach § 2 Abs. 3 Ziff. 4 DSFA-V verarbeitet werden und die Verarbeitung der personenbezogenen Daten gem. § 2 Abs. 3 Ziff. 1 DSFA-V umfangreich ist. Zwar bietet die DSGVO keine Definition, was unter einer ‚umfangreichen Verarbeitung' zu verstehen ist, im Sinne eines ordentlichen Risikomanagements sollte allerdings eine Datenschutz-Folgenabschätzung in betriebsratlosen Betrieben realisiert werden.[85]

F. Erstellung eines Löschkonzeptes

Ein weiteres Spannungsverhältnis der WBRL und der DSGVO manifestiert sich zwischen den Dokumentationserfordernissen nach Art. 18 WBRL und den Löschpflichten nach Art. 17 Abs. 1 DSGVO.[86]

Aus dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO sind Daten zu löschen, sobald diese nicht mehr benötigt werden.

schutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

84 Garante per la Protezione dei dati personali 9685922, abrufbar unter: https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9685922 (Stand: 15.12.2023).

85 Schweiger RdW 2020, 533 (535).

86 Fehr ZD 2022, 256 (260).

Sowohl die Datenschutzkonferenz[87] als auch die Art.-29-Datenschutzgruppe[88] sehen eine Frist von zwei Monaten nach Abschluss der Ermittlungen vor, nach der die personenbezogenen Daten zu löschen sind. Sind jedoch weitere rechtliche Schritte wie die Einleitung eines Strafverfahrens oder eines Disziplinarverfahrens notwendig, so kann die Speicherdauer ausgeweitet werden, während die Löschung nach Ende der Rechtsmittelfristen des Verfahrens durchzuführen ist.

In der Praxis kann dies problematisch werden, wenn es zu einem späteren Zeitpunkt, etwa durch eine weitere Meldung eines Hinweisgebers oder neue Informationen bekannt werden. Die DSGVO sieht hierfür eine einzige Ausnahme im Art. 17 Abs. 3 lit. e vor, sofern erst weitere rechtliche Schritte wie Disziplinarverfahren oder die Einleitung von Strafverfahren abgeklärt werden müssen. Dies gilt der Sicherung zur Geltendmachung eigener Rechtsansprüche sowie der Verteidigung gegen Rechtsansprüche von Dritten.[89]

Auf Basis dieser Ausnahme können personenbezogene Daten jedoch nicht immer bis zur Verjährungsfrist aufbewahrt werden. Um sich zulässigerweise auf die Ausnahme des Art. 7 DSGVO stützen zu können, wird dies mit einem bereits laufenden Verfahren zu begründen sein oder ein solches mit hinreichender Wahrscheinlichkeit zu erwarten sein. Wird mit keinen Verfahren in absehbarer Zeit gerechnet, sondern will das Unternehmen die Löschung nur aufschieben, weil es möglicherweise zu einem Rechtsstreit kommen könnte, wird im Einzelfall eine Interessensabwägung durchzuführen sein. Eine längere Speicherung der Daten wird demnach nur möglich sein, wenn konkrete Anhaltspunkte vorliegen, dass die Geltendmachung von Rechtsansprüchen oder deren Schwere gegenüber dem Eingriff in die Grundrechte des Betroffenen, der mit der Aufbewahrung verbunden ist, überwiegt.[90]

Eine Abhilfe für die Praxis bietet die Pseudonymisierung und Verschlüsselung der Daten nach Art. 32 Abs. 1 lit. a DSGVO. Die bereits abgearbeiteten Meldungen können von einer Art ‚Löschgruppe' mit den zuständigen Akteuren des Unternehmens aus den Compliance-, Datenschutz- und Per-

87 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

88 Artikel-29-Datenschutzgruppe WP 117, 14.

89 Fehr ZD 2022, 256 (260).

90 Altenbach/Dierkes CCZ 2020, 126 (129).

sonalabteilungen pseudonymisiert werden. In einem weiteren Schritt kann die pseudonymisierte Meldung archiviert werden, wobei eine Löschung zu einem späteren Zeitpunkt zwingend notwendig sein wird.[91]

Anstelle der Löschung können die Daten, wenn möglich und sinnvoll, auch anonymisiert werden, da die DSGVO auf diese nicht anwendbar ist und damit ein Wissensverlust von bisherigen Meldungen vermieden wird.[92]

§ 5 Arbeitsverfassungsrechtliche Aspekte bei der Umsetzung

Mit dem Einsatz von Hinweisgebersystemen kommt es zu einer weitreichenden Verarbeitung personenbezogener Daten der Beschäftigten. Diese Daten bergen das Risiko eines Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer. Aus diesem Grund sind Whistleblowing-Systeme nicht nur auf ihre datenschutzrechtliche, sondern ebenso auf ihre arbeitsverfassungsrechtliche Zulässigkeit zu prüfen.[93]

Aus der Sicht des Arbeitsrechts stellt sich bei der Einrichtung interner Whistleblowing-Kanäle die Frage, ob diese die Zustimmung des Betriebsrates durch eine Betriebsvereinbarung erfordern – oder jene der Arbeitnehmer, sofern kein Betriebsrat besteht.

A. Zustimmung des Betriebsrates

Nach der Bestimmung des § 96 Abs. 1 Ziff. 3 des Arbeitsverfassungsgesetzes (ArbVG) brauchen Kontrollmaßnahmen und technische Systeme, die auf die Kontrolle der Arbeitnehmer abzielen und die Menschenwürde berühren, zu ihrer Rechtswirksamkeit die Zustimmung des Betriebsrates.

In ihrer Spruchpraxis ging die Datenschutzbehörde davon aus, dass bei der Einrichtung von Whistleblowing-Kanälen zwingend immer eine Betriebsvereinbarung abgeschlossen werden muss. Während *Thiele/Wagner*[94] dieser Linie folgen und den Abschluss einer Betriebsvereinbarung als zwingend ansehen, da es sich um eine Kontrollmaßnahme handelt, die die

91 Fehr ZD 2022, 256 (260).
92 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 212.
93 Knyrim/Haidinger Praxishandbuch Datenschutzrecht S. 114.
94 Thiele/Wagner Umsetzung der DSGVO in der Personalpraxis S. 48.

Menschenwürde berührt, sind Teile der Lehre anderer Ansicht und üben scharfe Kritik an dieser Spruchpraxis. Demnach müsse bei der Einführung von Hinweisgebersystemen differenziert werden, ob diese die gesetzlichen Mindestinhalte überschreiten oder nicht. Hier kommt es bezüglich der Frage, ob eine Betriebsvereinbarung abgeschlossen werden muss, darauf an, ob die vorausgesetzten Tatbestandsmerkmale vorliegen. Im Falle der Einrichtung von Whistleblowing-Systemen sind hier die Tatbestände der Betriebsvereinbarung von Relevanz: einerseits der bereits angesprochene § 96 Abs. 1 Ziff. 3 ArbVG und andererseits § 96 a Abs. 1 Ziff. 1 ArbVG.[95]

Für personenbezogene Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und zu fachlichen Voraussetzungen hinausgehen, gilt Folgendes: Nach der genannten Bestimmung braucht die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung solcher Daten nur dann den Abschluss einer Betriebsvereinbarung, wenn die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht (§ 96a Abs. 1 Z 1 ArbVG).

Hier wird jedoch die Ansicht der Datenschutzbehörde, dass es sich bei Hinweisgebersystemen um Kontrollmaßnahmen nach § 96 Abs. 1 Ziff. 3 ArbVG handelt und nicht um Systeme zur Personaldatenverarbeitung, außen vorgelassen. Erfolgt die Subsumtion eines Hinweisgebersystems nämlich unter § 96 Abs. 1 Ziff. 3 ArbVG, so ist jedenfalls der Abschluss einer Betriebsvereinbarung verpflichtend – selbst dann, wenn die Errichtung des Meldesystems auf Grundlage einer gesetzlichen Verpflichtung erfolgt. Die Rechtsansicht der Datenschutzbehörde wird auch in diesem Punkt als inhaltlich zu undifferenziert kritisiert. Sofern nur bestimmte Verstöße, wie jene gegen das Unionsrecht, zu melden sind und nicht jegliches Fehlverhalten bekanntzugeben ist, das durch einen Arbeitnehmer gesetzt wird (zB eine Arbeitszeitverletzung oder Mobbing am Arbeitsplatz), erfüllt ein Hinweisgebermeldesystem wohl nicht die Voraussetzungen eines Kontrollsystems bzw. erlangt es nicht eine derartige Intensität, die bei Beschäftigten das Gefühl einer ständigen Überwachung auslöst.[96]

Schweiger[97] vertritt aufgrund der Tatsache einer gesetzlich verankerten Mindestausgestaltung eines Hinweisgebersystems die Ansicht, dass sich Unternehmen bei der Einführung interner Meldekanäle für Whistleblower auf

95 Zankl/Kühteubl/Pusch Rechtshandbuch der Digitalisierung Rn 69.
96 Zankl/Kühteubl/Pusch, Rechtshandbuch der Digitalisierung Kap. 13.
97 Schweiger RdW 2020, 533.

die Bestimmung des § 96 a Abs. 1 Ziff. 1 ArbVG berufen können. Damit bedarf ein Whistleblowing-System, das nur die gesetzlich vorgeschriebenen Mindestinhalte umsetzt und von Unternehmen auf Grund der Anzahl der Mitarbeiter oder der Branche eingerichtet werden muss, nicht der Mitwirkung des Betriebsrates.

Anderes gilt, wenn sich ein Unternehmen, das nicht der gesetzlichen Verpflichtung zur Einrichtung eines Whistleblowing-Systems unterliegt, die Entscheidung trifft, ein solches einzuführen. Dann wird jedenfalls die Mitwirkung des Betriebsrates benötigt. Wenn sich das Unternehmen jedoch hierbei nach den gesetzlichen Mindestmaßen richtet und nicht darüber hinausgeht, so ist nach Ansicht von *Schweiger* auch eine fakultative Betriebsvereinbarung nach § 97 Abs. 1 Ziff. 20 ArbVG in Betracht zu ziehen.[98]

Ob eine Betriebsvereinbarung abzuschließen ist, wird daher oft vom konkreten Einzelfall und den Ausgestaltungen des Systems abhängen. Wird im Betrieb ein Zustand der ständigen Kontrolle erreicht, weil die Beschäftigten vertraglich dazu verpflichtet sind, jegliches Fehlverhalten und jegliche Verstöße gegen interne Compliance-Richtlinien zu melden, und kommt es so zu einem „dauernden Spitzelwesen", so wird eine Betriebsvereinbarung zwingend notwendig sein.[99]

Bei einer Ausgestaltung der Hinweisgeberkanäle über die gesetzliche Mindestverpflichtung hinaus ist damit in allen Betrieben davon auszugehen, dass es sich hierbei um Kontrollmaßnahmen iSd § 96 Abs. 1 Ziff. 3 ArbVG handelt und eine zwingende Betriebsvereinbarung abzuschließen ist.

Aufgrund der verschiedenen Auswertungs- und Verknüpfungsmöglichkeiten wird jedoch teils auch die Meinung vertreten, dass es unwahrscheinlich ist, dass das Meldesystem sich stets innerhalb des gesetzlichen Rahmens bewegt, womit die Einrichtung des Whistleblowing-Systems immer auch die verpflichtende Mitwirkung des Betriebsrates braucht.[100] In ähnlicher Weise äußert sich ebenfalls die Judikatur des Obersten Gerichtshofes[101]. Demnach besteht eine Kontrollmaßnahme nach § 96 Abs. 1 Ziff. 3 ArbVG bereits, wenn die denkbare Möglichkeit eines Eingriffs in die Sphäre der Menschenwürde gegeben ist.

98 Schweiger RdW 2020, 533 (534).
99 Stella/Winter ZAS 2021/22, 124 (126).
100 Schweiger RdW 2020, 533 (534).
101 OGH 8 ObA 288/01p.

Stella/Winter[102] vertreten jedoch die Annahme, dass auch dann, wenn ein Hinweisgebersystem, das nur die Mindestanforderungen des Gesetzes erfüllt, dazu genutzt werden könnte, die Menschenwürde zu berühren, für den Betriebsinhaber die Möglichkeit der Einrichtung eines Meldesystems besteht – auch ohne die Zustimmung bzw. das Veto des Betriebsrates. Der Zweck der zwingenden Mitbestimmung des Betriebsrates besteht darin, die Gestaltungsmöglichkeiten von Arbeitgebern bei sensiblen Themen an die nur in bestimmten Fällen ersetzbare Zustimmung des Betriebsrates zu koppeln. Hat der Arbeitgeber jedoch gar nicht die Freiheit zur Gestaltung der Arbeitsbedingungen, sondern ist er durch den Gesetzgeber zu einem bestimmten Handeln verpflichtet, kann diese Pflicht nicht durch das Mitwirkungsrecht eines Betriebsrates umgangen werden. Durch die WBRL und die nationalen Umsetzungsakte der Mitgliedsstaaten werden Unternehmen ab einer bestimmten Mitarbeiteranzahl dazu verpflichtet, Hinweisgebersysteme mit gewissen Mindeststandards umzusetzen. Mit diesem Gesetz als lex specialis wird die betriebsverfassungsrechtlich verankerte Mitwirkung verdrängt.

Damit wird eine Betriebsvereinbarung nur dann notwendig sein, wenn das Unternehmen nicht gesetzlich dazu verpflichtet ist, ein internes Hinweisgebersystem einzurichten oder wenn dieses über die gesetzlich erforderliche Mindestausgestaltung hinausgeht.

Schweiger[103] nennt eine weitere Möglichkeit, um bei der Einführung von Whistleblowing-Systemen von einer die Menschwürde berührenden Maßnahme hin zu einem Personaldatensystem zu rücken: die Auslagerung des internen Meldekanals an einen Dienstleister, der sich gegenüber dem Unternehmen vertraglich dazu verpflichtet, die aus den Meldungen stammenden Informationen nicht zur Kontrolle der Mitarbeiter heranzuziehen, sondern sich rein im gesetzlichen Mindestmaß eines Hinweisgebersystems zu bewegen und Meldungen, die nicht in den sachlichen Anwendungsbereich fallen, nicht weiterzuverfolgen.

Als weitere Maßnahme, um das Berühren der Menschwürde der Arbeitnehmer zu verhindern, bietet sich das System der stufenweisen Kontrollverdichtung an. Hier wird der Zugriff auf die inhaltlichen Informationen einer Meldung in einer ersten Stufe auf eine technische Auswertung wie zB auf Schlagworte beschränkt. In einem nächsten Schritt erfolgt die Auswertung

102 Stella/Winter ZAS 2021/22, 124 (126).
103 Schweiger RdW 2020, 533 (534).

mit Bezug auf vorab festgelegte Zwecke, die in den Anwendungsbereich des Gesetzes fallen. Erst in der dritten Stufe sollen inhaltliche Ermittlungen in der Meldung unter der Verarbeitung von personenbezogenen Informationen möglich sein.[104]

B. Zustimmung der Arbeitnehmer

Sofern kein Betriebsrat vorhanden ist, muss bei der Einführung von internen Hinweisgebersystemen die schriftliche Zustimmung jedes einzelnen Arbeitnehmers gem. § 10 Abs. 1 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) eingeholt werden, wenn keine gesetzliche Pflicht zur Errichtung besteht oder die Ausgestaltung über die gesetzlichen Mindestanforderungen hinausgeht.[105] Nach § 10 Abs. 2 des AVRAG kann die Zustimmung des Beschäftigten, soweit eine schriftliche Vereinbarung mit dem Arbeitgeber über deren Dauer nicht vereinbart wurde, jederzeit ohne Einhaltung einer Frist schriftlich gekündigt werden. Im Fall der Verweigerung der Zustimmung oder deren Rücknahme dürfte das Whistleblowing-System nicht mehr auf diesen Arbeitnehmer anwendbar sein. Er darf also weder Hinweise geben noch dürfen diese in einer Meldung genannt werden.

§ 6 Der österreichische Umsetzungsakt der WBRL

Obwohl die Umsetzungsfrist zur WBRL am 17.12.2021 endete, ist die EU-Richtlinie erst im Februar 2023 dem Nationalrat zur Beschlussfassung vorgelegt worden und trat mit 25. Februar 2023 in Kraft.

A. Der Anwendungsbereich

Die WBRL lässt den Mitgliedsstaaten die Möglichkeit offen, den sachlichen Anwendungsbereich auf nationale Gesetze auszudehnen (vgl. Kap. 2.2). Diesen Spielraum hat Österreich in gewissem Ausmaß auch genutzt und Meldungen über Korruptions- sowie Amtsdelikte (§§ 302–309 StGB) in § 3 Abs 3 HSchG aufgenommen.

104 Kotschy/Reimer ZAS 2004, 167.
105 Neumayr/Reissner Zellkomm Rn 3.

Der § 28 Abs. 3 HschG schreibt eine Beurteilung der Wirkung des HSchG ab 2026 vor. Ziel dieser Regelungen ist es, auf Basis der Erfahrungen der folgenden Jahre die Ausdehnung der Geltungsbereiche im innerstaatlichen Recht zu erweitern.[106]

Auch laut dem allgemeinen Teil der Erläuterungen zum Gesetz sind spätere Erweiterungen des sachlichen Geltungsbereichs vorgesehen. Dies wird nach den künftigen Erfahrungen mit dem HSchG zu entscheiden sein. Weshalb dies aber erst zu einem späteren Zeitpunkt beschlossen werden soll, wird damit begründet, dass kleine und mittlere Unternehmen mit der Einrichtung eines neuen Hinweisgebersystems nicht zu stark belastet werden sollten.[107]

Bezüglich der Frage, welche Betriebe ein Whistleblowing-System verpflichtend einführen müssen, findet sich eine Präzisierung in § 11 Abs. 2 HSchG. Bei Unternehmen mit (saisonal) fluktuierenden Mitarbeiterzahlen wird laut § 3 Abs. 2 HSchG die durchschnittliche Anzahl der Mitarbeiter der drei personalstärksten Monate des vergangenen Kalenderjahres herangezogen, um festzulegen, ob diese einen internen Meldekanal einrichten müssen oder nicht.

B. Die Rechtsgrundlage

Das Gesetz bildet in § 8 Abs. 2 DSGVO die Rechtgrundlage für die Verarbeitung von personenbezogenen Daten aus Hinweisgebersystemen. Demnach kommt für Unternehmen, die in den Anwendungsbereich der Richtlinie fallen, die Rechtsgrundlage des Art. 6 Abs. 1 lit. c zum Tragen.

C. Anonyme Meldungen

Die WBRL verpflichtet die Mitgliedsstaaten nicht dazu, anonyme Hinweise zuzulassen (vgl. Kap. 2.3.4), doch wird die Möglichkeit der Anonymität für Hinweisgeber im Gesetz vorgesehen. Sollte deren Identität dennoch offengelegt werden, so sieht § 6 Abs. 3 HSchG vor, dass dem Hinweisgeber trotzdem der Schutz nach den Bestimmungen des HSchG garantiert ist.

Im Falle einer anonymen Meldung werden jedoch die Information an den Hinweisgeber über Folgemaßnahmen nach § 11 Abs. 9 HSchG oder

106 210/ME 27. GP Erläut 14.
107 210/ME 27. GP Erläut 1.

auch die Bestätigung des Gesprächsprotokolls mit Unterschrift gem. § 9 HSchG nicht möglich sein.

D. Konzerninterne Meldekanäle

Nach § 13 Abs. 4 HSchG besteht für Konzerne und Unternehmensgruppen die Möglichkeit, ein Whistleblowing-System gemeinsam zu betreiben und dieses auch einem externen Dienstleister auszulagern. Soweit ein gemeinsames Hinweisgebersystem betrieben wird, sieht das § 8 Abs. 3 HSchG vor, dass die Betriebe gemeinsam verantwortlich sind, gem. Art. 4 Ziff. 7 in Verbindung mit Art. 26 DSGVO.

Anders als in der WBRL sowie in den dazu verfassten Stellungnahmen der Europäischen Kommission (vgl. Kap. 2.3.5) gibt es jedoch keine gesetzlich vorgeschriebene Maximalanzahl von Beschäftigten, die das Betreiben einer gemeinsamen internen Whistleblowing-Stelle einschränkt. Damit wäre es auch für Großkonzerne mit Tochtergesellschaften über 250 Mitarbeiter möglich, gemeinsam ein Hinweisgebersystem zu betreiben. Zudem schreiben das nationale Gesetz sowie auch die WBRL ausdrücklich die Möglichkeit vor, Dritte mit dem Betrieb eines internen Meldekanals zu betrauen. Damit könnte ebenfalls eine Tochtergesellschaft im Konzernverbund mit dem Betrieb eines Whistleblowing-Systems für die anderen Gesellschaften beauftragt werden. Dies widerspricht jedoch der Ansicht der Art.-29-Datenschutzgruppe, wonach die Meldung vorrangig in jenem Mitgliedsstaat bearbeitet werden soll, in dem diese getätigt wurde (vgl. Kap. 3.3.2).[108]

Hier verabsäumte der Gesetzgeber es, mit einer ausreichend klaren Bestimmung Rechtsunsicherheiten völlig auszuräumen. Zu hoffen bleibt, dass im finalen Gesetzesentwurf oder in den Erläuterungen klargestellt wird, ob für Konzerne die zentrale Einrichtung einer Meldestelle ausreichend ist.

E. Datenschutzrechtliche Einschränkungen

In § 8 HSchG werden Einschränkungen des Datenschutzrechts zu Gunsten des Betriebs von Hinweisgebersystemen vorgesehen. Nach § 8 Abs. 1 HSchG dient die Verarbeitung der personenbezogenen Daten den Zwecken

108 Artikel-29-Datenschutzgruppe WP 117, 18.

des HSchG nach § 1 und § 8 Abs. 2 Ziff. 1. Hier wird jedoch offengelassen, welche Art der Datenverarbeitung vorgesehen werden kann.

Der § 8 Abs. 9 HSchG legt eine weitgehende Beschränkung der Betroffenenrechte nach Kapitel III DSGVO fest. Demnach muss ein Unternehmen den Betroffenen nach Art. 13 und 14 DSGVO nicht darüber informieren, dass eine Meldung über ihn eingegangen ist, und auch nicht seiner Auskunftspflicht gegenüber dem Betroffenen nach Art. 15 DSGVO nachkommen.

In den Gesetzesmaterialien finden sich jedoch keine Erläuterungen dazu, welcher Rechtsgrund des Art. 23 Abs. 1 lit. a bis j DSGVO die konkrete Beschränkung erfordert. Dies wurde im Begutachtungsverfahren vom Datenschutzrat als auch dem Bundesministerium für Justiz kritisiert, demnach sei eine Prüfung dahingehend notwendig, in welchem Ausmaß sowie für welche Zeitspanne die Beschränkung der Betroffenenrechte zur Zweckerreichung tatsächlich erforderlich ist. Die Beschränkungen konkretisiert und befristet werden.[109] Der Kritik dieser ausufernden Beschränkung der Betroffenenrecht wurde im HinSchG durch den Gesetzgeber nicht Rechnung getragen.

F. Datenschutz-Folgenabschätzung

Nach Art. 35 Abs. 10 DSGVO müssen Verantwortliche mit der gesetzlichen Verpflichtung nach dem Unionsrecht oder dem Recht des Mitgliedstaats zur Einrichtung eines Hinweisgebersystems keine eigene Datenschutz-Folgenabschätzung durchführen, sofern im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass des Gesetzes eine Datenschutz-Folgenabschätzung bereits erfolgte und es nach dem Ermessen des Mitgliedstaates nicht erforderlich ist. Demnach ist eine konkrete Datenschutz-Folgeabschätzung für die Einrichtung und den Betrieb eines Hinweisgebersystems ist vom Verantwortlichen nach § 8 Abs. 13 HSchG nicht durchzuführen, weil im Rahmen des Gesetzgebungsverfahren bereits eine allgemeine Datenschutz-Folgeabschätzung erfolgte.[110]

109 Datenschutzrat, Stellungnahme abrufbar unter, https://www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_221151/index.shtml (Stand: 15.12.2023); Bundesministerium für Justiz, Stellungnahme abrufbar unter https://www.parlament.gv.at/gegenstand/XXVII/SNME/221188/ (Stand: 15.12.2023).

110 210/ME 27. GP Erläut 9.

Auf diese Ausnahme kann sich eine Person jedoch nur berufen, wenn die Verarbeitung der personenbezogenen Daten auf der Rechtsgrundlage des Art. 6 Abs. 1 lit. c (Erfüllung einer rechtlichen Verpflichtung) oder lit. e (Wahrnehmung einer Aufgabe im öffentlichen Interesse) aufbaut. Erfolgt die Datenverarbeitung im Rahmen eines internen Meldekanals jedoch auf lit. f (berechtigtes Interesse), so ist demnach eine Datenschutz-Folgenabschätzung durchzuführen.

Kritik zu dieser beigelegten Datenschutz-Folgenabschätzung wurde im Rahmen des Begutachtungsverfahrens des Ministerialentwurfs unter anderem durch die Datenschutzbehörde und den Datenschutzrat kundgetan. Demnach sei die allgemeine Datenschutz-Folgenabschätzung zu pauschal gehalten, um den Vorgaben der DSGVO zu entsprechen. Besonders die Maßnahmen zur Datensicherheit sind zu wenig konkret und dürften vor allem für Verantwortliche, die nun ein Hinweisgebersystem einführen müssen, kaum eine Hilfe darstellen. Hier wird jedoch nur auf Art. 32 DSGVO verwiesen. Die Sicherheit der Verarbeitung, die in dieser Bestimmung geregelt wird, ist jedoch bei jeder Datenverarbeitung einzuhalten. Hier wäre es vielmehr sinnvoll gewesen, dem Stand der Technik entsprechende Maßnahmen anzuführen, um den verantwortlichen Stellen im Unternehmen einen Weg aufzuzeigen. Denkbar wäre hier etwa die Schulung der Mitarbeiter, die Hinweise bearbeiten, oder eine entsprechende Verschlüsselung der Meldekanäle.[111]

G. Die Aufbewahrungsfrist

Die Aufbewahrungsfrist, welche im Ministerialentwurf des Gesetzes vorgesehen war, stand in einem klaren Spannungsverhältnis zur DSGVO und konfligierte mit den Grundsätzen der DSGVO der Zweckbindung, der Datenminimierung und der Speicherbegrenzung von personenbezogenen Daten nach Art. 5 DSGVO.

Die vormals vorgesehen Aufbewahrungsfrist war mit dreißig Jahren ab der letztmaligen Verarbeitung und bei Protokolldaten sogar dreiunddreißig Jahre ab der letztmaligen Verarbeitung vorgesehen gewesen (§ 8 Abs. 9 -10 ME HSchG). Diese Aufbewahrungsfrist wicht damit vom Unionsrecht ab. Zwar können Einschränkungen der DSGVO nach Art. 23 DSGVO zulässig

111 Datenschutzbehörde, Stellungnahme abrufbar unter https://www.parlament.gv.at/PtWeb/api/s3serv/file/cb34b15b-dc74-4c93-90fb-b377813afb9b (Stand: 15.12.2023).

sein, diese müssen aber notwendig und verhältnismäßig sein, was bei Speicherfristen von bis zu dreiunddreißig Jahren fraglich ist.

Ausführungen in den Erläuterungen zum Gesetz, weshalb eine so lange Aufbewahrungsdauer gewählt wurde, gab es dazu nicht. Eine derart lange Frist wurde auch vom EU-Gesetzgeber nicht initiiert. Art. Art. 18 WBRL sieht vor, dass Meldungen nicht länger aufbewahrt werden sollten, als dies erforderlich und verhältnismäßig ist. Eine Verkürzung der Aufbewahrungsfrist scheint in Anbetracht dessen angemessen.

In den im § 3 Abs. 3 HSchG angeführten Bereichen, die in den sachlichen Anwendungsbereich des Gesetzes fallen, findet sich sogar nur selten eine Verjährungsfrist von bis zu zehn Jahren, wie bspw. die Geldwäschebestimmung gem. § 21 FM-GwG oder die Aufbewahrung ärztlicher Aufzeichnungen und Dokumentationen nach § 51 Abs. 3 ÄrzteG. Bei gemeldeten Verstößen, die sich gegen das Verwaltungsstrafrecht richten, gilt nach § 31 VStG lediglich eine Verjährungsfrist von drei Jahren.

Die lange Verjährungsfrist von dreißig Jahren nach § 1489 S. 2 ABGB, wenn dem Betroffenen der Schaden oder der Schädiger nicht bekannt wurden oder der Schaden aus einem Verbrechen entstanden ist, wird zumeist weder erforderlich noch verhältnismäßig sein.

Bei Meldungen, die sich als unrichtig herausstellen, wird eine Aufbewahrung zudem gar nicht notwendig sein. Eine Begründung zu dieser überaus langen Speicherfrist findet sich lediglich in der Datenschutz-Folgeabschätzung und lautet wie folgt: *„Diese Frist orientiert sich an der längsten für Verfahren der Rechtsdurchsetzung relevanten Verjährungsfrist."*[112]

Diese Begründung wird für die meisten Meldungen aus internen Hinweisgebersystemen, wie soeben dargelegt, nichtzutreffend sein und lässt außerdem die Ansicht der österreichischen Datenschutzbehörde außer Acht, wonach der Verantwortliche darlegen muss, *„welche konkreten zukünftigen Verfahren auf welcher Grundlage anhängig gemacht werden könnten und inwiefern durch derartige Verfahren eine Notwendigkeit zur weiteren Speicherung der personenbezogenen Daten begründet wird"*.[113]

In der Praxis würde dies aber mit einem äußerst hohen administrativen Arbeitsaufwand einhergehen. Der § 10 Abs. 6 sieht schließlich vor, dass diese Daten unter hohen Sicherheitsstandards *„in einem vertraulichen und sicheren System zu speichern"* (§ 10 Abs. 6 ME HSchG) sind. Eine so lange

112 210/ME XXVII. GP - Ministerialentwurf - Datenschutz-Folgenabschätzung.
113 DSB-D123.085/0003-DSB/2018, 27.08.2018.

Aufbewahrungsfrist pauschal festzulegen, würde zudem auch gegen den Sinn und Zweck eines Löschkonzeptes sprechen.

Aus diesem Grund folgte der Gesetzgeber in diesem Punkt den kritischen Stellungnahmen, welche während des Begutachtungszeitraums eingingen und die Aufbewahrungsfrist wurde unter § 8 Abs. 11 HSchG neu geregelt. Die vorgeschriebene Frist für personenbezogene Daten aus Hinweisgebersystemen beträgt fünf Jahre ab der letztmaligen Verarbeitung. Zudem sind personenbezogene Daten so lange aufbewahrt werden, wie es für laufende Verwaltungs-, Zivil- oder strafrechtliche Ermittlungsverfahren erforderlich ist.

Protokolldaten über Verarbeitungsvorgänge, wie etwa Änderungen, Abfragen und Übermittlungen, unterliegen einer gesonderten Aufbewahrungsfrist von drei Jahren über die übliche Aufbewahrungsdauer hinaus. Nach Ablauf dieser Aufbewahrungsfrist sind personenbezogene Daten zu löschen (§ 8 Abs. 12 HSchG). Personenbezogene Daten, die nicht für die Verarbeitung von Hinweisen erforderlich sind, dürfen nicht erhoben werden und müssen, sollten diese versehentliche erfasst werden unverzüglich gelöscht werden wie § 8 Abs. 10 HSchG festlegt.

H. Sanktionen

Die WBRL regelt in Art. 23, dass die Mitgliedstaaten bei der Umsetzung in nationales Recht wirksame Sanktionen festzulegen haben (vgl. Kap. 2.4.4). Dies findet sich im Entwurf des HSchG, wobei jedoch nicht über die Richtlinie hinausgegangen wird. Der § 24 HSchG sieht Strafbestimmungen für Personen vor, die Maßnahmen der Vergeltung gegen Hinweisgeber setzen, den Schutz der Vertraulichkeit verletzen und ebenso für Personen, die wissentlich einen falschen oder irreführenden Hinweis geben. Hierbei handelt es sich um eine Verwaltungsübertretung, die mit einer Geldstrafe von bis zu 20.000 Euro und im Wiederholungsfall bis zu 40.000 Euro zu ahnden ist. Eine Strafe für Unternehmen, die zwar der gesetzlichen Pflicht zur Einrichtung eines Whistleblowing-Systems unterliegen, dieser aber nicht nachkommen, gibt es lt. § 24 HSchG. nicht.

I. Übergangsfristen

Verpflichtet nach dem HSchG sind Unternehmen und juristische Personen des öffentlichen Bereichs ab mindestens 50 Mitarbeitenden. Unternehmen sind juristische Personen des Privatrechts sowie rechtsfähige Personengesellschaften. Damit sind auch Vereine und gemeinnützige Organisationen verpflichtet Meldekanäle zu implementieren und betreiben. Die Gesellschaft bürgerlichen Rechts sowie der der Einzelunternehmer sind damit ausgenommen. Ebenfalls in die Pflicht miteinbezogen sind juristische Personen des öffentlichen Sektors, wie Bund, Länder und Gemeinden.[114]

In § 28 HSchG hat der Gesetzgeber jedoch Übergangsfristen für die Einführungen der Hinweisgebersysteme vorgesehen.

Ab dem Inkrafttreten des Gesetzes gilt eine Übergangsfrist von sechs Monaten, somit bis zum 25.8.2023 für juristische Personen mit mindestens 250 Beschäftigten (§ 28 Abs. 1 HSchG).

Unternehmen mit weniger als 250 Arbeitnehmern wird eine Übergangsfrist bis zum 18.12.2023 gewährt (§ 28 Abs. 2 HSchG). Damit ist die Umsetzung der WBRL in Österreich zwei Jahre nach der Umsetzungsfrist der Europäischen Kommission für die Mitgliedstaaten, die am 17.12.2021 endete, vollzogen.

§ 7 Conclusio

Mit der Umsetzung der WBRL in innerstaatliches Recht durch das HSchG kann in Österreich der Anreiz zur Abgabe von Hinweisen und zum Schutz der Hinweisgeber geschaffen werden. Aber nicht nur für die hinweisgebende Personen bietet der Schutz vor Repressalien Vorteile, auch für Unternehmen hat die Einführung von integren Whistleblowing-Systemen einen klaren Mehrwert. Zwar mag die Sorge vor Denunzianten und einer Flucht von Hinweisen groß sein, die noch größere Chance, dadurch möglichen Verstößen intern aufzuklären und sich dadurch zu verbessern, bevor sich Hinweisgeber damit an externe Meldestelle oder die Öffentlichkeit wenden, sollte nicht verkannt werden.

Auch wenn der Handlungsspielraum, den die WBRL den Mitgliedstaaten in Bezug auf den sachlichen Anwendungsbereich offen lässt vom österreichischen Gesetzgeber, teils genutzt wurde und nationales Recht mit einbe-

114 Irresberger/Stangl-Krieger/Bruchbacher/Kercz/Wasinger GRCaktuell 2023, 28.

zogen wurde (vgl. Kap.5.1), so ist bei der Umsetzung in Unternehmen der Rahmen für mögliche Meldungen nicht zu streng nach dem Gesetz auszulegen. Vielmehr sollten weitere Hinweise zu nationalen Gesetzen oder internen Compliance-Policys zugelassen werden. Einerseits ist für den Hinweisgeber in manchen Fällen gar nicht abschätzbar, ob der Verstoß, den er melden will, nun beispielsweise das europäische oder nationale Vergaberecht betrifft. Andererseits ist es im Interesse des Unternehmens, Kenntnis über mögliches Fehlverhalten und Verstöße zu haben und dagegen intern vorgehen zu können.

Meines Erachtens wäre es daher sinnvoll, das Gesetz in Zukunft auf innerstaatliches Recht auszudehnen. Schließlich sind hier auch einzelne Bundesländer bei der Umsetzung der WBRL weitergegangen: Das Burgenländische Hinweisgeberschutzgesetz (Bgld. HSchG) erstreckt den sachlichen Anwendungsbereich auf alle Verstöße gegen Landesrecht (§ 3 Bgld. HSchG). So resultiert die Situation, dass erstens Beschäftigte bei einem Rechtsträger der öffentlichen Hand wie der burgenländischen Landesregierung einen viel umfassenderen Rechtsrahmen bei der Meldung von Verstößen haben als Arbeitnehmer im privaten Sektor im Burgenland. Zweitens kommt es damit in neun verschiedenen Landesgesetzen zum Hinweisgeberschutz und zusätzlich zu einem bundesweiten Gesetz, wobei alle nicht aufeinander ausgerichtet sind.

Für Unternehmen birgt der aktuell vorliegende Gesetzesentwurf zur Umsetzung der WBRL außerdem das Potential zu Konflikten mit dem Datenschutzrecht. Dies betrifft einerseits Unternehmen, die nun erstmalig einen internen Meldekanal einrichten, und andererseits Unternehmen, die ein bereits bestehendes zu adaptieren haben, um dieses gesetzeskonform zu betreiben.

Für Konzerne ist derzeit noch offen, ob ein zentraler gemeinsamer Meldekanal immer geführt werden kann oder ob jede Tochtergesellschaft dies dezentral zu organisieren hat. Hinzu kommt die Frage, wie mit Tochtergesellschaften umzugehen ist, die etwa weniger als 50 Mitarbeiter beschäftigen. Diese würden nicht in den Anwendungsbereich des Gesetzes fallen. Dabei gibt es für jeden Betrieb auch die Möglichkeit, freiwillig ein Whistleblowing-System zu führen. In diesem Fall gelten jedoch nicht die datenschutzrechtlichen Erleichterungen, die im Gesetz vorgesehen sind, wie die Beschränkungen der Betroffenenrechte nach Kapitel III der DSGVO. In einer Unternehmensgruppe würde dies bedeuten, dass kleine Tochtergesellschaften nicht an zentralen Meldekanälen teilnehmen dürften bzw. deren Meldungen datenschutzrechtlich anders zu behandeln wären.

Ein weiteres Problem bei der Umsetzung für Unternehmensgruppen stellt sich in der zu Aufbewahrungsfrist. Diese wird nicht von der WBRL vorgegeben, was heißt, dass jeder Mitgliedstaat diese im nationalen Gesetz festlegt. Bei länderübergreifenden Unternehmensgruppen würde dies eine unterschiedlich lange Aufbewahrungsfrist je nach Sitz der Gesellschaft bedeuten.

Sitzt die Konzernmutter etwa in Deutschland und die Tochter in Österreich, so müsste eine Meldung, die von einem Mitarbeiter in der österreichischen Gesellschaft getätigt wird, nach dem HSchG fünf Jahre ab der letzten Verarbeitung aufbewahrt werden. In Deutschland, wo sich die Konzernmutter befindet, ist die Meldung jedoch laut Gesetz für einen besseren Schutz hinweisgebender Personen Hinweisgeberschutzgesetz (HinSchG) bereits drei Jahre nach Abschluss des Verfahrens zu löschen, besagt § 11 (5) HinSchG. Dies stellt besonders bei gemeldeten Verstößen, die Konzerne in verschiedenen Mitgliedstaaten betreffen, eine Herausforderung dar und gilt auch für den Fall, dass die Ermittlungen nicht nur in jenem Land, in dem die Meldung erfolgte, aufgenommen werden, sondern ebenso in anderen Ländern. Werden die Fristen für die Aufbewahrung nach den unterschiedlichen innerstaatlichen Ländern alle beachtet, so muss dies auch bei der Erarbeitung des Löschkonzeptes und der Strukturierung des Berechtigungsmanagements beachtet werden. Aufbauend auf dem bereits genannten Beispiel müsste die Dokumentation zum Hinweis und zu den eingeleiteten Ermittlungen demnach bei der Konzernmutter in Deutschland nach drei Jahren gelöscht werden. Bei der österreichischen Tochter könnte der Hinweis aber noch zwei weitere Jahre gespeichert werden.

Ob die Einrichtung von zentralen Meldekanälen in einer Konzerngruppe gesetzlich möglich ist und falls ja, bis zu welcher Beschäftigtenanzahl dies vorgesehen ist, wurde auch mit Inkrafttreten des Gesetzes noch nicht abschließend geklärt. Die Europäische Kommission und die Art.-29-Datenschutzgruppe haben sich bereits gegen den Betrieb einer zentralen Meldestelle ausgesprochen, die auch in allen Verstößen die Ermittlungen durchführen sollte. In der Praxis hat der Betrieb einer zentralen Meldestelle in Konzernen viele Vorteile. Einerseits werden mit der Bündelung Kosten und Ressourcen gespart, andererseits kann sich eine Tochtergesellschaft auf den Betrieb des Hinweisgebersystems spezialisieren, sodass alle Verbundunternehmen den Meldekanal an eine Gesellschaft auslagern. Dort kann sich eine eigene Compliance-Abteilung mit der Aufklärung und der Prüfung der Meldungen beschäftigen. Darüber hinaus ist es in der Praxis oftmals bereits der Fall, dass Unternehmensgruppen ein gemeinsames

Whistleblowing-System betreiben. Sollte diese Möglichkeit gesetzlich nicht ausreichend sein, so müssten diese auf dezentrale Kanäle umgestellt werden oder es sind neben dem bereits bestehenden zentralen Meldesystem noch zusätzliche Kanäle einzuführen.

Kompliziert kann es vor allem werden, wenn ein Mitgliedstaat den sachlichen Anwendungsbereich im Umsetzungsakt, wie dies die WBRL erlaubt, auf nationales Gesetz ausweitet. Diesen Handlungsspielraum hat der österreichische Gesetzgeber teilweise genutzt und auch Korruptions- sowie Amtsdelikte in das HSchG aufgenommen.

Dies würde jedoch zu folgendem Szenario führen: Ein Konzern mit Sitz der Muttergesellschaft in Deutschland hat Töchtergesellschaften in verschiedenen EU-Ländern, darunter ebenfalls in Österreich und Italien. Die italienische Tochtergesellschaft wurde damit beauftragt, einen zentralen Meldekanal für den gesamten Konzern zu implementieren und die Ermittlungen durchzuführen. Erfolgt nun aber eine Meldung von Beschäftigten der österreichischen Tochtergesellschaft über ein Korruptionsdelikt nach StGB, so müsste die italienische Schwesterngesellschaft eine sachverhaltsaufklärende Überprüfung nach dem Recht eines anderen Mitgliedstaates realisieren.

Neben den soeben beschriebenen Rechtsunsicherheiten für Konzerne kann es mit der Umsetzung der WBRL in nationales Recht auch für Kleinunternehmen, die nicht durch die gesetzliche Pflicht gebunden sind, ein Hinweisgebersystem zu implementieren, weil sie etwa weniger als 50 Mitarbeitende beschäftigte, dies aber freiwillig umsetzen möchten, zu Stolpersteinen kommen. Da sie nicht dem HSchG unterliegen, kommen ebenfalls die im Gesetz vorgesehenen Erleichterungen im Datenschutzrecht für die Einführung der Meldekanäle für sie zur Anwendung. Dies bedeutet, juristische Personen, welche nicht in den Anwendungsbereich des HSchG fallen, sollten bei der Einführung eines Whistleblowing-Systems jedenfalls eine Datenschutz-Folgenabschätzung durchführen, sofern kein Betriebsrat vorhanden ist und eine Betriebsvereinbarung nach der DSFA-V vorliegt. Ein Berufen auf die Beschränkung der Betroffenenrechte der DSGVO ist demnach auch nicht möglich.

Auf Grund des abgesteckten sachlichen Anwendungsbereichs auf das Unionsrecht und in Österreich ebenfalls auf das Korruptionsstrafrecht können sich Meldestellen bei Verstößen, die über die in § 3 HSchG genannten Rechtsbereiche hinausgehen, nicht auf das Gesetz stützen und würden für diese Bereiche wiederum freiwillig ein Hinweisgebersystem betreiben. Dies würde bedeuten, die Datenverarbeitung muss auf Art. 6 Abs. 1 lit. f DSGVO

gestützt werden. Für alle Verstöße, die nicht unter § 3 HSchG fallen, gelten damit auch nicht die datenschutzrechtlichen Erleichterungen nach dem HSchG.

Damit werden österreichische Unternehmen zudem vor Herausforderungen gestellt, wenn es um die Frage der Betroffenenrechte nach Kapitel III der DSGVO geht. In Folge wäre der Beschuldigte also nach Art. 14 und 15 DSGVO von der Verarbeitung seiner personenbezogenen Daten durch den gemeldeten Verstoß zu informieren und die Identität des Whistleblowers müsste somit offengelegt werden. Dies würde wiederum gegen Ziel und Zweck der WBRL sprechen und für Unternehmen mit einem hohen Verwaltungsaufwand einhergehen.

Hier werden sehenden Auges zwei verschiedene datenschutzrechtliche Regime geschaffen: einerseits jenes, für das die gesetzliche Deckung durch das HSchG gilt, und andererseits für alle Betriebe sowie Rechtsbereiche, die nicht dem Gesetz unterliegen. Diese Zweigleisigkeit ist aus praktischer und datenschutzrechtlicher Sicht bedenklich und könnte darüber hinaus zu einer Art ‚Zwei-Klassengesellschaft von Hinweisgebern' führen, wenn ein Hinweisgeber nicht unter den Schutz fallen würde, den das Gesetz bietet.

Um diese Pattsituation aufzulösen, könnte der Gesetzgeber vorsehen, die Möglichkeit der freiwilligen Unterwerfung in das HSchG zu integrieren. Damit wäre einerseits für die Kleinunternehmen mit bis zu 50 Mitarbeitern Abhilfe geschaffen, die interne Meldekanäle einführen wollen, und ebenso für eingehende Meldungen, die nicht Verstöße nach § 3 HSchG betreffen.

Aus arbeitsrechtlicher Sicht wird für Betriebe mit Betriebsrat bei der Umsetzung von Whistleblowing-Systemen wohl eine positive Zusammenarbeit notwendig sein. Nicht zuletzt kann die Aufklärung von Verstößen nicht nur für die Unternehmensführung, sondern ebenso für die Belegschaft Vorteile mit sich bringen, weshalb mit einer Sensibilisierung und Aufklärung aller Mitarbeiter schon vor der Einführung eines Meldekanals versucht werden sollte, in allen Unternehmensebenen Akzeptanz für Hinweisgebersysteme zu schaffen.

Tatsächlich lässt sich festhalten, dass auf die datenschutzrechtlichen Aspekte bei der Umsetzung der WBRL und der zukünftigen Einführung der internen Meldekanäle in Unternehmen nicht ausreichend Rücksicht genommen wurde und sich dadurch Spannungsverhältnisse ergeben.

Letztendlich ist abzuwarten, wie die Umsetzung mit der längsten Frist 17.12.2023 in österreichischen Unternehmen gelingt und neuen praktischen Erfahrungswerten und Erkenntnisse diese in die Evaluierung der Bestimmungen des HSchG durch den Gesetzgeber im Jahr 2026 einbezogen wer-

den, um hier vorhersehbaren Problemen durch gesetzliche Lösungen einen Riegel vorzuschieben.

Literaturverzeichnis

Altenbach/Dierkes EU-Whistleblowing-Richtlinie und DSGVO, CCZ 2020, 126.

Arnol, Whistleblower-Richtlinie und Gold Plating, GesRZ 2020, 153.

Artikel-29-Datenschutzgruppe Leitlinien für Transparenz gem. VO 2016/679 (WP 260 rev.01).

Artikel-29-Datenschutzgruppe Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität. WP 117.

Block/Kremer Whistleblowing im Konzern: Eine zentrale Stelle ist zu wenig! https://www.cmshs-bloggt.de/compliance/whistleblowing-im-konzern-eine-zentrale-stelle-ist-zu-wenig/. (15.8.2022).

Brodil Arbeitnehmerdatenschutz und Datenschutz-Grundverordnung (DSGVO), ecolex 2018, 486.

Brunner/Nagel Whistleblowing - Sicherstellung des Hinweisgeberschutzes, Datenschutz Konkret 2020, 32.

Council of Europe Protection of Whistleblowers, Recommendation CM/Rec (2014)7 and explanatory memoran-dum, https://rm. coe.int/16807096c7 (15.8.2022).

Datenschutzkonferenz Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf.

Dilling Der Schutz von Hinweisgebern und betroffenen Personen nach der EU-Whistleblower-Richtlinie, CZZ 2019, 214.

Ehrbar Whistleblowing - das Hinweisgebersystem im österreichischen Recht, NetV 2016, 20.

Europäisches Parlament Entwurf einer legislativen Entschließung des europäischen Parlaments, https://www.europarl.europa.eu/doceo/document/A-8-2018-0398_DE.html#title1 (15.8.2022).

Falter Whistleblower (un)erwünscht? in *Roters/Gräf/Wollmann* (Hrsg), Zukunft Denken und Verantworten. Herausforderungen Für Politik, Wissenschaft und Gesellschaft Im 21. Jahrhundert (2020) 353.

Fassbach/Hülsberg Beschäftigtendatenschutz im Hinweisgeberverfahren: Interessenkonflikt zwischen Hinweisgeberschutz und Auskunftsrecht des Beschuldigten, GWR 2020, 255.

Fehr Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld? ZD, 256–261.

Feiler/Rieken/Romandy Kapitel 3: Datenschutzkonforme Gestaltung von Hinweisgebersystemen, in *Petsche* (Hrsg), Whistleblowing & Internal Investigations. Praxiskommentar zur Whistleblowing-Richtlinie (2021).

Fleischer/Schmolk Finanzielle Anreize für Whistleblower im Europäischen Kapitalmarktrecht? NZG, 361.

Haidinger Kap 16, in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020).

Hastenrath ZHAW-Studie: Auswirkungen der Whistleblowing-Richtlinie, CB 2022, 58.

Fidler/Winner in Kalss/Oppitz/U. Torggler/Winner, BörseG/MAR § 124 BörseG (Stand 1.8.2019, rdb.at)

Irresberger, Stangl-Krieger, Bruchbacher, Kercz, Wasinger, Spezialfragen zur gesetzeskonformen Einrichtung von HinweisgeberInnensystemen, GRCaktuell 2023, 28.

Kotschy/Reimer Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 167.

Kröll/Stumpf Die EU-Richtlinie zum Schutz von Whistleblowern - Handlungsbedarf für Unternehmen, RdW 2020, 161.

Kühling/Buchner Datenschutz-Grundverordnung BDSG. Kommentar[4] (2024).

Kühteubl/Pusch Kap 13, in Rechtshandbuch der Digitalisierung (2021).

Moos Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit, in Moos/Schefzig/Arning/Baumgartner/Braun/Cornelius/Gardyan-Eisenlohr/Gausling/Hansen-Oest/Heinemann (Hrsg), Praxishandbuch DSGVO. Einschließlich BDSG und spezifischer Anwendungsfälle[2] (2021).

Neumayr/Reissner, Zeller Kommentar zum Arbeitsrecht[3] (2018).

Novacek, EU-RL zum Schutz der Hinweisgeber auf Verstöße gegen Unionsrecht ("Whistleblower") EU-RL zum Schutz der Hinweisgeber auf Verstöße gegen Unionsrecht ("Whistleblower")- Auswirkungen im Steuerrecht, FJ 2019, 222.

Paal/Pauly/Ernst, DS-GVO BDSG // Datenschutz-Grundverordnung. Bundesdatenschutzgesetz[3] (2021).

Peitsch, Whistleblowing-Hotlines spätestens 2021 verpflichtend. Bislang keine Pflicht zur Einrichtung von Whistleblowing-Hotlines, NetV 2020, 60.

Petsche, Kapitel 2: Rechtlicher Rahmen für Internal Investigations, in *Petsche* (Hrsg), Whistleblowing & Internal Investigations. Praxiskommentar zur Whistleblowing-Richtlinie (2021) 220.

Pollirer, Checkliste Whistleblowing, Dako 2020, 38.

Reppelmund, Whistleblowing-Richtlinie: Vorläufige Einigung zwischen Europäischem Parlament und den Mitgliedstaaten, EuZW 2019, 307.

Schmolke, Die neue Whistleblower-Richtlinie ist da! Und nun? NZG 2020, 5.

Schweiger, Die Richtlinie zum Schutz von Hinweisgebern - arbeitsrechtliche Konsequenzen (Teil II), RdW 2020, 533.

Stella/Winter, Whistleblowing-RL: Ungelöste Rechtsfragen für die betriebliche Umsetzung, ZAS 2021, 124.

tagesschau, Gründer von WikiLeaks: London bestätigt Auslieferung von Assange an die USA (17.6.2022).

Teichman/Weber, Die Whistleblowing-Richtlinie, ihr Missbrauchspotential und Implikationen für Compliance-Beauftragte, CB 2022, 157.

Thiele/Wagner, Umsetzung der DSGVO in der Personalpraxis. Fragen, Antworten, Muster (2019).

Zankl, Rechtshandbuch der Digitalisierung (2021).

Rechtsquellenverzeichnis

Arbeitsverfassungsgesetz BGBl 1974/22

Arbeitsvertragsrechts-Anpassungsgesetz BGBl 1993/459

Burgenländisches Hinweisgeberschutzgesetz LGBl. 26/2022

Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz – HSchG) BGBl. I Nr. 6/2023

Ministerialentwurf betreffend Bundesgesetz, mit dem ein Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz – HSchG) erlassen wird

Richtlinie des Europäischen Parlaments und des Rates v. 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl L 305/17.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119.

The False Claims Act

Dodd-Frank Wall Street Reform and Consumer Protection Act

Sarbanes-Oxley Act of 2002

Judikaturverzeichnis

OGH 13.6.2002, 8 ObA 288/01p.

DSB-D123.085/0003-DSB/2018, 27.8.2018.

LAG Baden-Württemberg, 20.12.2018, 17 Sa 11/18.

EGMR 16. 2. 2021, 23922/19, *Gawlik/Liechtenstein.*

VG Köln, 25.3.2022, 25 K 2138/19.