Vom »staatlich regulierten Verpfeifen« – zugleich Klarstellungen zu den Hinweisgebersystemen im liechtensteinischen Bankrecht

Nicolas Raschauer*

Abstract

Die Finanzmarktaufsicht (FMA) Liechtenstein sowie Banken und Wertpapierfirmen müssen nach FL-BankG sog »angemessene Verfahren« bzw ein »wirksames Meldesystem« einrichten, über das potentielle Verstösse gegen einschlägige Regelungen des Finanzmarktrechts gemeldet werden können. Wie diese Systeme auszugestalten und welche Rahmenbedingungen dabei zu beachten sind, ist unklar – Gesetz, Schrifttum und Rechtsprechung haben bislang viele Fragen offen gelassen. Das verwundert nicht, waren doch die einschlägigen Bestimmungen des BankG noch nicht Gegenstand vertiefter wissenschaftlicher Auseinandersetzung.

Der StGH hat jedoch in seinem Grundsatzurteil vom 3. September 2018 (StGH 2018/074) die Bedeutung dieser »Hinweisgebersysteme« im Hinblick auf das Grundrecht der Meinungsäusserungsfreiheit (Art 10 Abs 1 EMRK;[1] Art 40 LV[2]) deutlich gemacht; letztere ist Massstab für die Beurteilung der Frage, unter welchen Voraussetzungen »Hinweisgeber« extern Meldungen erstatten dürfen (»Whistleblowing«).[3]

Vor diesem Hintergrund erörtert das nachfolgende Manuskript – soweit ersichtlich erstmalig – Zweck, Grenzen und Bedeutung dieser »Hinweisgebersysteme« im liechtensteinischen Finanzmarktrecht.

1 Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten, LGBl 1982.060.001.
2 Verfassung des Fürstentums Liechtenstein vom 5. Oktober 1921 (LV), LGBl 1921.015.
3 Dazu *Dworschak/N. Raschauer*, »Whistleblowing« – Grundrechtliche Weichenstellungen in Liechtenstein, im Druck.

Schlagworte

Bank, Wertpapierfirma, Whistleblowing, Hinweisgebersystem, Hinweisgeber, Meinungsfreiheit

Rechtsquellen

Art 22, 64a BankG, Art 71 RL (EU) 2013/36, Art 73 RL (EU) 2014/65/EU

Inhaltsübersicht

* Das nachfolgende Manuskript basiert bereichsweise auf meiner Kommentierung zu § 99g ö BWG, die in aktualisierter Fassung bereits in *Laurer/Kammel/Ratka/Schütz*, BWG[4] (2020, rdb.at) veröffentlicht wurde, sowie auf meinem Einleitungsbeitrag »Whistleblowing« , der im gleichnamigen Tagungsband (hrsg von *Gruber/N. Raschauer*) 2014 im Manz Verlag erschienen ist. Das Manuskript wurde auf die liechtensteinische Rechtslage adaptiert und aktualisiert. Geringfügig aktualisierte Version vom 1.7.2020.

I. Einführung: Whistleblowing und Hinweisgebersysteme

»**Whistleblowing**« ist längst kein juristisches Phänomen mehr, sondern anerkanntes Mittel zur Korruptionsbekämpfung.[1] Aufgrund des damit einhergehenden Spannungsverhältnisses zwischen der Preisgabe geheimer Informationen und zweckmässiger Aufdeckung von Missständen bleibt »Whistleblowing« ein Reizwort.

»Whistleblowing«, aus dem Englischen »*to blow the whistle*« (»die Pfeife blasen«), gemeint »**jemanden verpfeifen**«,[2] knüpft sowohl semantisch als auch sinngemäss an ein wenig tugendhaftes Attribut an: Es setzt **Geheimnisverrat** und damit **Vertrauensbruch**, etwa gegenüber Dienstgebern oder Vertragspartnern, voraus.[3] Inwieweit eine solche Verletzung einer Verschwiegenheitspflicht zweckdienlich, notwendig und letztlich mit einer modernen Corporate Governance vereinbar ist, setzt pro Anlassfall eine diffizile Wertentscheidung und Interessenabwägung voraus.[4] Die begriffliche Konnotation des »Whistleblowing« durchlief einen steten Wandel.[5] Im Schrifttum finden sich Stimmen, die für eine neutrale Begriffswahl eintreten.[6]

Die rechtlichen Parameter, anhand derer die Zulässigkeit des »Whistleblowing« in Liechtenstein zu vermessen ist, bleiben jedoch weitgehend unscharf. Einerseits finden sich (etwa in unmittelbar anwendbaren EWR-Sekundärrechtsakten[7]) normative Gebote zur Einrichtung von **Hinweisgebersystemen**, andererseits fehlen – abseits rezenter judikativer Weichenstellungen – nach wie vor einheitliche gesetzliche Standards, anhand derer die Zulässigkeit von »**Whistleblowing**« beurteilt werden kann. Es ist daher ungeachtet der grundrechtlichen Rahmenbedingungen, die in einem gesonderten Manuskript beleuchtet werden,[8] angezeigt, die bestehenden finanzmarktrechtlichen Rahmenbedingungen für das »Verpfeifen« zu erörtern.

II. Ausgewählte Rechtsgrundlagen: Einrichtung von Hinweisgebersystemen

Die Begriffe »Whistleblowing« sowie »Whistleblower« sind im liechtensteinischen Recht **nicht legal definiert**. Lediglich **Art 71 Bst e DSG**[9] erwähnt den »**Hinweisgeber**« als besondere Kategorie des von der Verarbeitung personenbezogener Daten Betroffenen, ohne hingegen gleichzeitig eine Definition anzubieten.[10] Da es in Liechtenstein somit an einer einschlägigen Legaldefinition fehlt, ist zunächst die vom StGH in seiner Rsp entwickelte Begriffsdeutung heranzuziehen.

Der **StGH** umschreibt »Whistleblower« , bezugnehmend auf die im Schrifttum vertretene Begriffsklärung,[11] als »*Arbeitnehmer* (…), *der schwerwiegende Missstände in seinem Arbeitsumfeld aufdeckt und dabei primär aus uneigennützigen Motiven handelt*.« [12] Die aufgedeckten Missstände können sich bspw auf strafrechtlich relevantes Fehlverhalten von Mitarbeitenden in Finanzintermediären beziehen.[13]

Wortwörtlich ist Whistleblowing bis dato im liechtensteinischen Recht nicht verankert; wie eingangs erwähnt findet sich lediglich im DSG eine Bezugnahme auf »Hinweisgeber«.

A. Hinweisgebersysteme de lege lata

Allerdings enthält das nationale Finanzmarktrecht zahlreiche normative Vorgaben über »**Hinweisgeber-**

1 Vgl statt vieler die Beiträge in *Gruber/N. Raschauer* (Hrsg), Whistleblowing (2014).

2 *N. Raschauer*, Begriffsabgrenzung, in Gruber/N. Raschauer (Hrsg), Whistleblowing (2014) VI.

3 *Rieder*, Whistleblowing als Menschenrecht, jusletter 28.11.2011, Rz 1; *Ascher*, Whistleblowing – zwischen Denunziantentum und Zivilcourage, in Feiler/Raschhofer (Hrsg), Innovation und internationale Rechtspraxis (2009) 23 f; *Lewisch*, *Whistleblowing* und Strafrecht, in ÖDIP und OJV (Hrsg), Whistleblowing – das Hinweisgebersystem im österreichischen Recht (2012) 24 (25), demzufolge Whistleblower-Hotlines häufig pejorativ als »Vernaderungshotlines« etikettiert werden.

4 *Dworschak/N. Raschauer*, »Whistleblowing« , im Druck.

5 Etwa <https://www.vaterland.li/region/international/Liechtenstein-will-Whistleblower-schuetzen;art102,36475> (abgerufen am 23.3.2020).

6 *Huber*, Der Arbeitnehmer als Whistleblower, ASoK 2011, 255 (257) mwN, plädiert für eine »*Übersetzung des Begriffs ›Whistleblowing‹ mit einem nicht negativ besetzten neutralen ›Alarmschlagen‹*« .

7 Vgl zB Art 32 MAR (VO [EG] Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über *Marktmissbrauch* [Marktmissbrauchsverordnung], ABl 2014 L 173/1, EWR-Register Anh IX Ziff 29a.01). Dazu *Lins/N. Raschauer*, Art 32 MAR in Gruber (Hrsg), BörseG (2020, im Druck).

8 Vgl statt vieler die Beiträge in *Gruber/N. Raschauer* (Hrsg), Whistleblowing (2014).

9 Datenschutzgesetz (DSG) vom 4. Oktober 2018, LGBl 2018.272.

10 StGH LES 2018, 236 (239 f).

11 *Pabel*, Der grundrechtliche Schutz von Whistle-Blowing, in Feik/Winkler (Hrsg), FS Berka (2013) 161 (162); *Berka*, Whistleblower und Leaks. Von den Schwierigkeiten, das Amtsgeheimnis zu wahren in ÖJK (Hrsg), Recht und Öffentlichkeit. 40 Jahre ÖJK (2004) 71 f.

12 Art 5 Nr 7 der neuen EU-Whistleblowing-RL 2019/1937 enthält eine knappe Definition für den Begriff »Hinweisgeber« . Darunter wird »*eine natürliche Person (verstanden), die im Zusammenhang mit ihren Arbeitstätigkeiten erlangte Informationen über Verstösse meldet oder offenlegt*.« (RL [EU] 2019/1937 des Europäischen Parlaments und des Rates v 23.10.2019 zum Schutz von Personen, die Verstösse gegen das Unionsrecht melden [kurz »Whistleblowing-RL«], ABl 2019 L 305, 17).

13 *Berka,* aaO.

systeme« .[14] So hat etwa die **FMA Liechtenstein**[15] in Erfüllung ihrer gesetzlichen Aufgaben (Art 5 FMAG[16]) und in Durchführung EWR-rechtlicher Vorgaben (zB Art 71 Abs 1 CRD IV,[17] Art 73 Abs 1 MiFID II) ein **externes Hinweisgebersystem** eingeführt.[18] **Banken und Wertpapierfirmen** müssen **interne Meldesysteme** einrichten, die Mitarbeitenden offen stehen (Art 22 Abs 2 Bst e BankG).

Eine nähere Definition für »Hinweisgebersysteme« oder »Whistleblowing« sucht man in den Aufsichtsgesetzen indes vergeblich. Für die Einführung interner Meldesysteme (also »Hinweisgebersysteme«) wird im Normtext auf sog »**angemessene Verfahren**« abgestellt, die liechtensteinische Finanzintermediäre zur Missstandsmeldung zu etablieren haben. Die Einrichtung angemessener Verfahren, über die Mitarbeitenden/Angestellten dieser Institute etc die Möglichkeit zur Meldung von Verstössen gegen die einschlägigen Materiengesetze über einen »speziellen, unabhängigen und autonomen Kanal« eröffnet werden, ist jeweils als **Bewilligungsvoraussetzung** für Banken, Wertpapierfirmen,[19] geregelte Märkte,[20] MTF und OTF,[21] den Betrieb von Verwaltungsgesellschaften nach dem UCITS-G,[22] Alternative Investmentfondsmanager,[23] Vermögensverwalter nach dem VVG,[24] für Zentralverwahrer,[25] ua[26] gesetzlich vorgeschrieben.

Unabhängig davon schreibt Art 28a Abs 3 SPG[27] **Sorgfaltspflichtigen**[28] vor, »*über angemessene Verfahren (zu) verfügen, über die ihre Beschäftigten Verstösse nach Abs. 1 (Anmerkung: …) intern über einen speziellen, unabhängigen und anonymen Kanal melden können*«; der Normtext knüpft allerdings an ein quantitatives Element, da die Einrichtung eines solchen Meldesystems nur verbindlich ist »*sofern sie 100 oder mehr Beschäftigte haben, die an Geschäftsbeziehungen mitwirken.*«

B. Umsetzung von Unionsrecht

Aus der genannten Gruppe von Rechtsnormen, welche die FMA und andere Unternehmen zur Einführung von Hinweisgebersystemen verpflichten, sind hier stellvertretend **Art 22 Abs 2 Bst e** und **Art 64a Abs 1 BankG** herauszugeben. Die Bestimmungen wurden in Umsetzung des **Art 71 CRD** bzw des **Art 73 Abs 1 MiFID II** erlassen.[29]

Nach diesen Bestimmungen haben »die **zuständigen Behörden**« über wirksame und verlässliche **Mechanismen** zu verfügen, um zur **Meldung von** drohenden oder tatsächlichen **Verstössen** gegen die nationalen Vorschriften zur Umsetzung der CRD, gegen die CRR, die MiFID II bzw die MiFIR bei den »zuständigen Behörden«

14 Vgl bereits *Hauser*, Das Bild von Whistleblowing in der österreichischen Versicherungswirtschaft, ÖBA 2009, 497 (500); zur österreichischen Rechtslage auch *Majcen*, FMA-Whistleblowing-Hinweisgebersystem: Sind alle Hinweise zulässig? ÖBA 2014, 486; *N. Raschauer*, § 99g Rz 1 ff; ferner *Lins/N. Raschauer*, Art 32 MAR Rz 1 ff. Zur Entwicklung zB *Gruber*, Whistleblowing im Kapitalmarktrecht in Ennöckl ua (Hrsg), FS B. Raschauer (2013) 131.

15 Auch in Österreich hat die FMA ab 1.1.2014 ein IT-gestütztes Hinweisgebersystem eingerichtet.

16 Gesetz vom 18. Juni 2004 über die Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz), LGBl 2004.175.

17 Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (CRD IV), ABl 2013 L 176, 338 (EWR-Register Anh IX-14.01). Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl 2014 L 173, 349 (EWR-Register Anh IX-31ba.01).

18 Vgl Art 64a Abs 1 BankG (Gesetz vom 21. Oktober 1992 über die Banken und Wertpapierfirmen [Bankengesetz], LGBl 1992.108). S auch ErwG 64 und Art 35 Abs 1 der Versicherungsvertriebsrichtlinie (EU) 2016/97 (IDD) und dessen Umsetzung in Liechtenstein durch Art 73 Abs 1 VersVertG, LGBl 2018.009.

19 Art 22 Abs 2 Bst e BankG: »*Banken und Wertpapierfirmen benötigen: (…) lit e:* ***angemessene Verfahren****, über die Mitarbeiter Verstösse gegen dieses Gesetz und die Verordnung (EU) Nr. 575/2013 intern über einen* ***speziellen, unabhängigen und autonomen Kanal*** *melden können.*« (Hervorhebungen d Verf).

20 Art 30s Abs 1 Bst e BankG.

21 Art 30t Abs 1 Bst c BankG.

22 Art 21 Abs 3a UCITS-G (Gesetz vom 28. Juni 2011 über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren, LGBl 2011.295): »*Eine Verwaltungsgesellschaft muss über* ***angemessene Verfahren****, üb er die ihre Angestellten tatsächliche oder potenzielle Verstösse gegen dieses Gesetz und die dazu erlassenen Verordnungen intern über einen speziellen, unabhängigen und autonomen Berichtsweg melden können, verfügen.*«

23 Art 38 Abs 3 AIFMG (Gesetz vom 19. Dezember 2012 über die Verwalter alternativer Investmentfonds, LGBl 2013.049): »*Ein AIFM muss über angemessene Verfahren, über die seine Angestellten tatsächliche oder potenzielle Verstösse gegen dieses Gesetz und die dazu erlassenen Verordnungen intern über einen speziellen, unabhängigen und autonomen Berichtsweg melden können, verfügen.*«

24 Art 6 Abs 1 Bst n VVG (Gesetz vom 25. November 2005 über die Vermögensverwaltung [Vermögensverwaltungsgesetz], LGBl 2005.278) sieht als Bewilligungsvoraussetzung für Vermögensverwalter »***angemessene Verfahren*** *(vor) (…), über die Mitarbeiter Verstösse (…) intern über einen speziellen, unabhängigen und autonomen Kanal melden können.*«

25 Art 12 Abs 1 EWR-Zentralverwahrer-Durchführungsgesetz (EWR-ZVDG), LGBl 2017.426: »*Zentralverwahrer haben nach Massgabe von Art. 65 Abs. 3 der Verordnung (EU) Nr. 909/2014 angemessene Verfahren einzurichten, über die ihre Angestellten tatsächliche oder mögliche Verstösse gegen die Verordnung (…) intern melden können.*« . Abs 2 leg cit betrifft das externe Meldesystem bei der FMA.

26 Art 19 Abs 1 EWR-Wertpapierprospekt-Durchführungsgesetz (EWR-WPPDG), LGBl 2019.159: »*Emittenten, Anbieter oder die Zulassung zum Handel an einem geregelten Markt beantragende Personen haben nach Massgabe von Art. 41 Abs. 4 der Verordnung (EU) 2017/1129 angemessene Verfahren einzurichten, über die ihre Angestellten tatsächliche oder mögliche Verstösse gegen die VO (…) intern melden können.*«

27 Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz), LGBl 2009.047.

28 Das sind, neben den gängigen Finanzinermediären, auch Rechtsanwälte, Immobilienmakler, die Post oder Spelbanken (Art 3 Abs 1 SPG).

29 Vgl BuA 2017/14, 118; BuA 2014/67, 59.

zu ermutigen (Abs 1). Diese Mechanismen müssen bestimmte Voraussetzungen erfüllen (vgl zB Art 71 Abs 2 Bst a–d CRD).

Davon ist Art 71 Abs 3 CRD zu unterscheiden, demgemäss auch »**Institute**« (Art 4 Abs 1 Z 3 CRR), also EWR-Kreditinstitute und CRR-Wertpapierfirmen über »angemessene Verfahren« verfügen müssen, über die ihre Mitarbeiter **Verstösse** intern über einen speziellen, unabhängigen und autonomen Kanal **melden** können. Nicht davon erfasst sind andere Finanzintermediäre wie Versicherungsunternehmen.

Dem EWR-Finanzmarktaufsichtsrecht[30] kommt somit eine Vorreiterrolle zu, als es sowohl die zuständige nationale Aufsichtsbehörde als auch Banken und Wertpapierfirmen verpflichtet, ein sog »**Hinweisgebersystem**« zu implementieren, wodurch die Aufdeckung von Missständen und Gesetzesverstössen erleichtert werden soll.[31]

C. »Hinweisgebersystem« – Zweck

Der Begriff »Hinweisgebersystem« ist, wie gezeigt wurde, an die international gebräuchliche Bezeichnung »**Whistleblowing**« angelehnt. Es zielt auf die **Sammlung** verschiedener personenbezogener **Daten** und Informationen über **Rechtsverletzungen** jedweder Art durch eine zuständige unternehmens- bzw behördeninterne Stelle ab.[32] Hinweisgebersysteme haben sich mittlerweile, neben »klassischen« amtswegigen Ermittlungen, als effizientes Instrument zur Verfolgung von Rechtsverletzungen etabliert. Dadurch soll die Verfolgung von Verwaltungsübertretungen und gerichtlich strafbaren Vergehen/Verbrechen effektuiert wird.[33] »*Dies ist naheliegend, denn gerade Kapitalmarktdelikte können durch staatliche Stellen oft nur schwer entdeckt werden. Unternehmensangehörige sind kostengünstige und gut unterrichtete Informationssammler.*«[34]

Ein Hinweisgebersystem stellt ein institutionalisiertes, regelmässig elektronisches Verfahren zur Erfassung von Meldungen über rechtswidriges Verhalten dar. In der Praxis sind zwei Varianten dieser Systeme zu unterscheiden (was sich auch aus der Textierung des BankG ableiten lässt): **Behörden-** bzw **unternehmens-**/konzern**interne** Systeme und **externe Systeme,** die Hinweise (Anzeigen, Meldungen etc) erfassen.[35] Diese Systeme dienen der Sammlung personenbezogener Daten und Informationen. Die zuständige Stelle soll die Daten hinsichtlich relevanter Verdachtsmomente auswerten und den Verdacht gegebenenfalls an die Unternehmensleitung oder an sonstige Einrichtungen weiterleiten, die ein Ermittlungsverfahren durchführen. Dadurch wird ein Verfahren zur Überprüfung der Verdachtsmomente in Gang gesetzt.

Ziel dieser Systeme ist die Sicherstellung der »**Compliance**« der Marktteilnehmer, der Mitarbeiter von Finanzintermediären und dergleichen.[36] Dadurch soll der Gehorsam von Mitarbeitern eines Finanzintermediärs genauso sichergestellt werden wie allgemein die Einhaltung massgeblicher Rechtsvorschriften durch diese Institute. Beides kann durch bestehende Ermittlungsbehörden bzw unternehmensinterne Überwachungssysteme allein (offensichtlich) nicht sichergestellt werden. Hinweisgebersysteme sollen daher Private und Marktteilnehmer ermutigen, Missstände im Betrieb oder in ihrem Umfeld zu melden. Die Systeme zielen darauf ab, die Sanktionierung von Regelverletzungen sicherzustellen und sollen Missständen präventiv entgegenwirken.

Bei einem Hinweisgebersystem handelt es sich um eine **Datenanwendung,** für die die Standards der **DSGVO**[37]

30 Manchmal verpflichten auch Rechtsvorschriften eines Drittstaates zur Einrichtung eines Hinweisgebersystems (was hier nicht zu vertiefen ist). In diese Kategorie fällt zunächst der US-amerikanische Sarbanes Oxley-Act, der die Finanzberichterstattung für börsennotierte Unternehmen in den USA regelt und daher auch für liechtensteinische Tochterunternehmen US-amerikanischer Gesellschaften verbindlich ist. Zudem hatte die ehemalige ö DSK 2013 einen Fall einer österreichischen Tochter eines deutschen Grosskonzerns zu beurteilen. Sie hielt fest, dass der deutsche Corporate-Governance-Kodex – also anerkannte Leitlinien für die verantwortungsvolle Führung und Leitung eines Unternehmens –, die nach § 161 des deutschen AktG verbindlich sind, die verpflichtende Einrichtung eines Hinweisgebersystems rechtfertige (vgl ö DSK 30.4.2013, K600.322–005/0003-DVR/2013). Das alles darf nicht darüber hinwegtäuschen, dass für die Implementierung eines solchen Systems in Liechtenstein immer noch die Schranken der nationalen bzw der EWR-Rechtsordnung beurteilungserheblich sind.

31 Dabei sind Hinweisgebersysteme nicht neu, wenn man an venezianische, namentlich am Dogenpalast angebrachte »Beschwerdebriefkästen« (»boche di leone«) denkt.

32 Vgl zB *Kutschera*, Whistleblowing – Überlegungen de lege lata et ferenda, in Fitz (ua), Hrsg FS Hellwig Torggler (2013) 697.

33 Die Bedeutung der angesprochenen Systeme zeigt sich anhand folgender »Kennzahlen« zum ö BKMS®-Hinweisgebersystems der ö WKStA (§ 2a Abs 6 ö StAG): Mit Stand 31.5.2014 erfolgten 117.813 Zugriffe auf das Hinweisgebersystem (das sind, seit Inbetriebnahme des Systems, täglich rund 269 Zugriffe). Zum genannten Stichtag langten 1747 Anzeigen bei der StA via BKMS ein. Von diesen Meldungen betrugen 29,82 % Korruptionsdelikte, 28,71 % Finanzstrafsachen, 22,87 % Wirtschaftsstrafsachen und 13,34 % Sozialbetrug (Zahlen laut *Haslwanter,* Anonyme Hinweisbearbeitung mit dem BKMS®-Hinweisgebersystem in der Praxis der Wirtschafts- und Korruptionsstaatsanwaltschaft in *Gruber/N. Raschauer,* Whistleblowing 13). Bei der FMA Ö gingen 2017 158 Hinweise zu Fehlverhalten auf dem österreichischen Finanzmarkt ein (Presseaussendung der FMA vom 19.4.2018).

34 *Heidinger/Strauss*, Whistleblowing im Kapitalmarktrecht, in *Gruber/N. Raschauer,* Whistleblowing 61.

35 Vgl auch ErläutRV 2438 BlgNR 24. GP 64 (§ 99g ö BWG).

36 Vgl auch *Lehner/Reisenberger* in *Dellinger,* Bankwesengesetz (8. Lfg 2016) § 99g Rz 1: Ziel sei es, eine hohe Gesetzestreue in den Kreditinstituten zu erreichen, um allfällige Gefährdungen von Instituten durch die Nichtbefolgung der im G verwiesenen Bestimmungen hintanzuhalten.

37 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen

gelten. Der Verantwortliche (Art 4 Nr 7 DSGVO) hat, anders gewendet, das System ein Einklang mit der DSGVO zu organisieren und zu betreiben. Insb hat er die erforderlichen »technisch-organisatorischen Massnahmen« gem Art 24 ff; 32 DSGVO nach dem einschlägigen Stand der Technik zu implementieren, um das System datenschutzkonform handhaben zu können. Zudem sind der Verantwortliche, seine Mitarbeiter sowie seine Auftragsdatenverarbeiter (Art 4 Nr 8 DSGVO) zur Einhaltung des Datengeheimnisses verpflichtet (Art 26 DSG).

Aus datenschutzrechtlicher Sicht sind regelmässig zwei weitere Themenstellungen von Bedeutung. Einerseits die **Verarbeitung personenbezogener Daten** (Art 4 Nr 2; Art 5 ff DSGVO) durch den Verantwortlichen eines Hinweisgebersystems und seine Auftragsdatenverarbeiter. Andererseits die **Weitergabe der Daten** an »Dritte« (etwa externe Ermittlungsbehörden), zB im Wege einer Anzeige gem § 53 StPO. Auf Basis der übermittelten Daten kann der »Dritte« – etwa die StA – diese Daten zu spezifischen Zwecken (weiter)verwenden, etwa indem er konkrete Untersuchungsschritte im Verdachtsfall setzt.[38]

Im Anschluss sind nun die beiden Arten von Hinweisgebersystemen, wie sie im BankG reguliert werden, näher zu untersuchen.

III. Behördliches Hinweisgebersystem

A. Allgemeines

In Umsetzung der Art 71 Abs 1 CRD, Art 73 Abs 1 MiFID II iVm Art 64a Abs 1 BankG hat die **FMA** ein externes **Hinweisgebersystem** eingerichtet. Damit wurde das gesetzliche Gebot, dass die nationalen Aufsichtsbehörden über »wirksame Mechanismen zu verfügen [haben], die dazu ermutigen, Verstösse [...] anzuzeigen« , auf Ebene der FMA umgesetzt.[39]

Personen, die Kenntnis von einem Verstoss gegen ein der FMA zur Aufsicht übertragenes Gesetz haben oder diesbezüglich einen begründeten Verdacht hegen, haben die Möglichkeit, der Behörde entsprechende Hinweise postalisch oder elektronisch, per Mail, zu übermitteln.

Die konkrete technische **Ausgestaltung** des Hinweisgebersystems obliegt an sich dem Ermessen der **Behördenleitung,** in der FMA daher der Geschäftsleitung (Art 17 FMAG). Sie hat das System anhand der relevanten Delikte (»Meldethemen«), die von einer Meldung betroffenen Personen, das anzuwendende Verfahren der Informationsweitergabe, die Meldestelle, die zur Empfangnahme eines Hinweises berechtigten Personen sowie die technisch-organisatorische Ausgestaltung des Systems (Art 24 ff und 32 DSGVO) exakt zu determinieren. Insgesamt ist die tatsächliche Ausgestaltung von Hinweisgebersystemen an der Aufgabenstellung und den Kapazitäten des behördlichen Wirkungsbereichs der FMA anzupassen, weshalb auch die datenschutzrechtliche Zulässigkeit des Systems nicht abstrahiert von einem konkreten Sachverhalt beurteilt werden kann.

Die FMA Liechtenstein hat sich durch die Bekanntgabe einer E-Mailadresse und einer postalischen Zustelladresse für ein »simples Meldesystem« entschieden.[40] Einen anderen Weg ist die ö FMA gegangen. Sie hat sich für den Einsatz jenes elektronischen Systems (»**BKMS®-Hinweisgebersystem**«) entschieden, das auch die ö WKStA seit 2013 anwendet.[41] Das elektronische Hinweisgebersystem ist über die Website der FMA zugänglich. Den anonymen Hinweisgebern wird durch den Einsatz moderner Sicherheits- und Verschlüsselungstechniken eines datenschutzzertifizierten Hinweisgebersystems Datensicherheit und Vertraulichkeit garantiert. Über diese Plattform ist auch ein anonymer Dialog mit den Hinweisgebern zur weiteren Abklärung der Informationen möglich.[42]

In beiden Fällen ist eine gesonderte »Anmeldung« oder Prüfung des Hinweisgebersystems bei der/durch die jeweils zuständige/n Datenschutzbehörde nicht erforderlich; wohl aber ist die nationale Finanzmarktaufsicht (als Betreiberin des Hinweisgebersystems) verpflichtet, die Vorgaben der DSGVO zu erfüllen, dh das System datenschutzkonform zu betreiben (Art 4 Nr 7; 24 ff, 32 DSGVO).

B. Anforderungen an das Hinweisgebersystem

1. Wirksamkeit/Verlässlichkeit

Das von zu der FMA zu betreibende Hinweisgebersystem soll »**wirksam**« und »**verlässlich**« sein (Art 64a Abs 1 BankG).[43] Zudem soll es dazu ermutigen, Verstösse anzuzeigen.

bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl 2016 L 119, 1 (EWR-Register Anh XI-5e.01).

38 Davon ist der Fall zu unterscheiden, in dem der Verantwortliche (zB die FMA) die via Hinweisgebersystem verarbeiteten Daten für andere legitime behördliche Zwecke, etwa für ein Verwaltungsstrafverfahren, weiterverwendet (Art 6 Abs 1 Bst c DSGVO).

39 <https://www.fma-li.li/de/kundenschutz/meldung-von-gesetzes verstossen.html>, abgerufen am 3.6.2020.

40 Es wurde daher ein »allgemein zugänglicher, sicherer Berichtsweg« implementiert (Art 64a Abs 1 BankG).

41 Näher zur Funktionsweise dieses Systems *Haslwanter* in *Gruber/N. Raschauer,* Whistleblowing 13 ff.

42 So die Selbstdarstellung der FMA unter <https:// www.fma.gv.at/oesterreichs-finanzmarktaufsichtsbehoerde-fma-schaltet-whistleblower-hotline-frei/>, zuletzt abgerufen am 20.3.2020.

43 Die entsprechende, in Art 71 CRD IV enthaltene Wortfolge »verlässlich« wurde zB in § 99g ö BWG nicht »übernommen« und ist daher im Zweifel, da die Begriffe nicht deckungsgleich sind, zum Begriff »wirksam« hinzuzulesen (in der englischen Sprachfassung verlangt die CRD IV »effective and reliable mechanisms«).

Der Begriff »**wirksam**« ist im Kontext des Zieles des Hinweisgebersystems zu interpretieren. Das System ist, etwa aus Sicht der Benutzerfunktionalität, derart zu konzipieren und zu gestalten, dass Meldungen über drohende oder tatsächliche Rechtsverstösse möglichst einfach und ohne grössere Hürden, ggf anonym erstattet werden können, ohne dass sich der Anzeigende gefährden könnte.[44] Dadurch soll die Compliance auf dem Finanzmarkt effektuiert werden; behauptete Verstösse sollen umfassend überprüfbar sein. Das System muss daher für jedermann leicht auffindbar sein. Daher ist es folgerichtig, wenn die FMA auf der Webseite auf das Hinweisgebersystem verlinkt. Im Hinblick auf die Zielsetzung des Art 71 CRD und des Art 64a Abs 1 BankG sollte die FMA als Betreiber des Systems potenziellen Benutzern auch Hilfestellungen und Erläuterungen über die Funktionalität des Systems zur Hand geben.

Zusätzlich soll das System »**verlässlich**« sein. Es sollte daher technisch ausgereift (dem Stand der Technik entsprechend) gestaltet sein (Art 24 ff, 32 DSGVO), möglichst rasch aufgerufen werden können (das System muss daher betriebsbereit gehalten werden, wenngleich nicht »rund um die Uhr«) und derart strukturiert sein, dass Daten und Informationen entsprechend den gesetzlichen Vorgaben »sicher« verarbeitet werden (dabei müssen die Grundsätze des Art 5 DSGVO gewahrt werden). Insb muss das System gewährleisten, dass zB die Privatsphäre der Anzeigeleger gewahrt bleibt (Art 8 Abs 1 EMRK[45]).

Wenn das System zusätzlich **ermutigen** soll, **Verstösse anzuzeigen,** mangelt es dem BankG an weiterführenden Anordnungen, die dieses Kriterium – analog etwa der ö Kronzeugenregelung des § 209a ö StPO – konturieren.[46] Im Zweifel ist dem Gesetzgeber zu unterstellen, dass er schon in der Einrichtung eines Hinweisgebersystems durch die FMA von einem insoweit »ermutigenden Ansatz« ausgehen dürfte.

2. »Spezielle Verfahren«

Gem Art 64a Abs 2 Bst a BankG sind im Hinweisgebersystem »**spezielle Verfahren**« für den Empfang der Meldungen über Verstösse und deren Weiterverfolgung vorzusehen (s dazu noch unten im Text). Gemeint ist zweierlei:

- Eine **Funktion,** welche es Personen ermöglicht, Mitteilungen bzw **Anzeigen** – ggf inklusive Beilagen – ohne grösseren Aufwand **an die FMA zu übermitteln;** die Behörde muss in der Lage sein, Informationen und Unterlagen möglichst einfach zu speichern, zu analysieren und weiterzuverarbeiten.
- Eine **Funktion,** die es der Behörde in die Lage versetzt, im Einzelfall **Zweifelsfragen,** die im Lauf der Ermittlungen auftreten, mit dem Anzeigeleger rasch nach Meldungslegung **abzuklären** (**Postfachfunktion**).

Diese »Verfahren« sind derart zu gestalten, dass erforderlichenfalls auch erforderliche »**Begleitdaten**« mitprotokolliert und gespeichert werden können, soweit dies mit Abs 2 Bst b und c vereinbar ist (zB wer zu welchem Zeitpunkt eine Anzeige eingebracht hat, welche Unterlagen der Anzeige angeschlossen wurden etc).

Mit »speziell« ist idZ nicht nur die Funktionalität der Verfahren gemeint, sondern auch die **technische Gestaltung** des Systems. Es ist derart einzurichten, dass es sich – im Hinblick auf Abs 2 Bst c – auf dem Stand der Technik befindet (man denke etwa an Verschlüsselung und dergleichen), um eine sichere und effektive Kommunikation zwischen Behörde und Hinweisgeber zu ermöglichen und die Geheimhaltung des Hinweisgebers zu wahren.[47]

In weiterer Folge hat die FMA verschiedene **Folgemassnahmen** zu entwickeln, verbindlich festzuschreiben und anzuwenden, welche die Behörde und ihre Mitarbeitenden in die Lage versetzen, Hinweise auszuwerten und daran anknüpfend die erforderlichen (Ermittlungs)Schritte zu setzen. Es sind daher Schritte zu entwickeln, die klarstellen, wer Berichte auszuwerten hat, wie sie evaluiert werden und unter welchen Voraussetzungen Folgeschritte gesetzt werden (näher unten im Text).

3. Schutz des Hinweisgebers

Dem **Schutz des Betroffenen** einer Meldung wird in Art 64a BankG wenig Aufmerksamkeit zuteil; zwar wird der Schutz des Anzeigelegers in drei Buchstaben des Abs 2 – richtlinienbedingt – thematisiert; allerdings lassen

44 Man denke an drohende arbeits-, zivil- oder strafrechtliche Konsequenzen.

45 Im Licht von StGH 2018/074 ist davon auszugehen, dass Art 8 EMRK nicht nur durch die FMA als ermittelnde und sanktionierende Behörde unmittelbar zu beachten ist, sondern dieses Grundrecht auch mittelbar inter privatos (also etwa für Banken und ihre Mitarbeitenden und die Angezeigten) von Bedeutung ist. Die einfachgesetzlichen Bestimmungen des BankG über Hinweisgebersysteme sind daher konventionskonform anzuwenden.

46 Besondere Anreize dahingehend, dass einem Hinweisgeber Straffreiheit oder -milderung zugesichert wird, können von der FMA derzeit mangels Ermächtigung nicht gewährt werden.

47 Dieser Aspekt kann hier nur skizziert werden: Vor der Implementierung des Systems ist daher klarzustellen, dass das System keine IP-Adressdaten, Cookies, Zeitstempel oder Metadaten speichern darf, soweit daraus Rückschlüsse auf den Hinweisgeber möglich sind. Ferner, inwieweit Daten, die eingemeldet werden, verschlüsselt werden bzw inwieweit das System, das zum Einsatz gelangt, überprüft wird (zu denken ist – im Hinblick auf Art 24 ff DSGVO – ua an Aspekte der Sicherheitszertifizierung) etc.

sich die Anordnungen auf eine zentrale Verhaltenspflicht der FMA als Auftraggeberin des Hinweisgebersystems reduzieren. Im Gegensatz zu Art 32 MAR (VO [EU] 596/2014), der die Wahrung der Vertraulichkeit der Identität des Hinweisgebers während aller Phasen des Ermittlungsverfahrens (und wohl auch darüber hinaus) verlangt, fordert Art 64a Abs 2 BankG (insb Bst b und c) – im Sinne eines Grundsatzes – »nur« die **relative Geheimhaltung** der Identität des Hinweisgebers.[48]

Die **Pflicht zur Geheimhaltung** der Identität des Hinweisgebers (vgl auch Art 31a BankG) basiert auf dem Umstand, dass sich der Hinweisgeber durch eine Anzeige zivil-, arbeits- und strafrechtlichen Sanktionen sowie **Vergeltungsmassnahmen** aussetzen könnte. Immerhin könnte er Treuepflichten gegenüber seinem Arbeitgeber verletzen, die unter anderen in verschiedenen Gehorsams- und Geheimhaltungspflichten zum Ausdruck kommt (zB Art 14 Abs 1 BankG; § 1173a Art 4 Abs 4 ABGB und dergleichen).

Aus Art 64a Abs 2 Bst c iVm Art 31a BankG folgt, dass die FMA, was den Betrieb des Hinweisgebersystems und die darin verarbeiteten Daten anlangt, grds zur Geheimhaltung verpflichtet ist. Das Gesetz verlangt allerdings **keinen absoluten Schutz der Identität des Hinweislegers.** Die FMA ist berechtigt, personenbezogene Daten über diesen zu verarbeiten (zB Name; Funktion; Adresse und dergleichen), wenn ihr diese Daten freiwillig übermittelt/offengelegt werden.[49] Die Behörde ist aber auch ermächtigt, die Daten des Hinweisgebers an Dritte weiterzugeben, soweit dies gesetzlich vorgesehen und im Anlassfall, etwa für die Einvernahme als Zeuge in einem gerichtlichen Strafverfahren, unbedingt erforderlich ist (Art 64 Abs 2 Bst c BankG; s auch § 53 StPO und andere Anzeigetatbestände).[50]

Der gesetzlich angeordnete Schutz erfasst sowohl **natürliche** als auch **juristische Personen** und Personengesellschaften, ungeachtet von Staatsangehörigkeit, Sitz, Rechtsform udgl (Art 8 Abs 1 EMRK).

Aus Sicht des Hinweisgebers bedeutet dies: Will er seine **Anonymität** wahren, hat er selbst sicherzustellen, dass keine personenbezogenen Daten gegenüber der FMA offengelegt werden (etwa in Beilagen). Vice versa hat die FMA keine Befugnis, einen Hinweisgeber – der sich via Hinweisgebersystem an die Behörde wendet – zur Preisgabe seiner Daten zu zwingen. Erfolgt dies jedoch freiwillig, ist die Behörde berechtigt, die offenbarten Daten zu speichern und weiterzuverarbeiten (s zB Art 6 Abs 1 Bst c DSGVO; Art 22 Abs 1 FMAG).[51]

Um die Geheimhaltung des Hinweisgebers zu gewährleisten, folgt aus Art 64a Abs 2 Bst c BankG, dass die FMA intern **klare Regeln** zu erstellen und anzuwenden hat.[52] Darunter fällt zunächst die Pflicht der Behördenmitarbeitenden zur Wahrung der Verschwiegenheit (Art 31a FMAG). Die Behörde ist verpflichtet, **adäquate Datensicherheitsstandards** gem Art 24 ff; 32 DSGVO nach dem aktuellen Stand der Technik zu implementieren.[53] Die FMA hat in internen Leitlinien[54] festzulegen, welche Mitarbeiter der Behörde Zugriff auf das System und die in weiterer Folge gespeicherten Daten und Informationen erhalten. Es ist ferner klarzustellen, für welche Zwecke Daten verwendet werden dürfen. Der Zugriff auf die Daten wie auch die weitere Verwendung ist zu protokollieren und dergleichen.

In Anlehnung an die Auffassung der ehem »Artikel-29-Datenschutzgruppe« (nunmehr Ausschuss gem Art 63 DSGVO) – zuvor ein beratendes Gremium der Europäischen Kommission nach der RL 95/46/EG – könnte die FMA zudem folgende Massnahmen setzen:[55]

- Strikte **Trennung** der mit der Bearbeitung von Meldungen betrauten Stelle von anderen Behördeneinheiten (Sicherstellung von Verschwiegenheitsbereichen – »chinese walls«-Prinzip);
- **Einschränkung des Anwendungsbereichs** des Hinweisgebersystems auf bestimmte relevante Deliktsgruppen (Verhinderung des »Denunziantentums«);
- **Löschung eingemeldeter Daten** spätestens zwei Monate nach Beendigung der Untersuchung, soweit sich nicht aus gesetzlichen Vorschriften eine längere Aufbewahrungspflicht ergibt.

48 Arg aus Art 64a Abs 2 Bst c BankG: *»Schutz der personenbezogenen Daten … für die Person, die die Verstösse anzeigt.«*

49 Es besteht daher kein gesetzliches Verwertungsverbot.

50 Die entsprechende Auflistung des Art 64a Abs 2 BankG ist unvollständig, da es mitunter erforderlich sein kann, die Identität einer Person auch gegenüber anderen Institutionen (zB der Geschäftsprüfungskommission des Landtages) offenzulegen. Auch wenn dies im Gesetz nicht berücksichtigt wurde, wäre eine entsprechende Offenlegung von Details gegenüber dem Landtag durch Art 23 ff GVVKG gedeckt.

51 Beachte die beschränkten Informationspflichten der FMA qua Art 12 ff DSGVO iVm Art 23 FMAG.

52 Auch nach der Rsp der ö DSB ist der Auftraggeber eines Hinweisgebersystems verpflichtet, adäquate und wirksame (insb auch technische) Rahmenbedingungen im System vorzusehen, um ein Gleichgewicht zwischen den konfligierenden Interessen der Meldungsleger, der Verdächtigen und des Auftraggebers herzustellen (so zB ö DSK 14.12.2012, K600.320–005/0003-DVR/2012 – *N-Company*).

53 Zieht die FMA einen Auftragsdatenverarbeiter zum Betrieb des Hinweisgebersystems heran (Art 28 DSGVO), bleibt die FMA im Aussenverhältnis dennoch für die Einhaltung der Sicherheitsstandards verantwortlich (Art 5 Abs 2; 82 Abs 2 DSGVO). Zwischen FMA und Auftragsdatenverarbeiter ist eine schriftliche Vereinbarung zu schliessen, die den zwingenden Vorgaben des Art 28 Abs 3 DSGVO entsprechen muss.

54 Damit dieser »Verhaltenskodex« wirkt, sollte er für die betroffenen Mitarbeiter der Behörde – etwa durch einen Passus im Dienstvertrag – für verbindlich erklärt werden.

55 Vgl <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf>, zuletzt abgerufen am 20.3.2020. Überarbeitete Leitlinien des Europäischen Datenschutzausschusses gem Art 63 DSGVO zu diesem Thema bestehen derzeit nicht.

4. Schutz der Tatverdächtigen

Neben dem Hinweisgeber unterliegt auch jede **Person**, die **mutmasslich »für einen Verstoss verantwortlich ist«** (daher jeder Tatverdächtige[56]) einem – wenngleich eingeschränkten – Schutz (Art 64a Abs 2 Bst c BankG). Die FMA hat daher auch diesbezüglich »Massnahmen« vorzusehen, welche den **Schutz der Identität** der Tatverdächtigen gewährleisten, wenngleich der Schutz nur eingeschränkt zu gewährleisten ist. Das ergibt sich unter anderem daraus, dass (Verwaltungs)strafverfahren regelmässig nur gegen einen **konkreten Tatverdächtigen** geführt werden (Art 139 ff LVG[57]). Bedenkt man aber, dass Hinweisgebern in diesen Verfahren regelmässig keine Parteistellung (und nicht notwendigerweise die Stellung eines Zeugen) zukommt, hat die FMA in Einklang mit Art 31a und Art 64a Abs 2 Bst c BankG sowie Art 8 Abs 2 EMRK sicherzustellen, dass die Identität des Tatverdächtigen nur dann gegenüber Dritten offengelegt wird, wenn dies im jeweiligen Kontext unbedingt erforderlich ist (s auch Art 5 Abs 1 DSGVO).

Nach dem Wortlaut des Art 64a Abs 2 Bst c BankG sind jedoch nur jene **natürlichen Personen** (dh Tatverdächtige) geschützt, die »mutmasslich für einen Verstoss verantwortlich« sind. Daraus folgt zunächst, dass Daten über Personen, die nicht idS mutmasslich tatverdächtig sind, nicht als Verdächtige geführt werden dürfen; Daten über diese Personen dürfen nur dann (weiter) verarbeitet werden, wenn ihnen eine spezifische Rolle in einem Ermittlungsverfahren zukommen könnte (zB als Zeuge).

Dass Art 64a Abs 2 BankG nur natürlichen Personen einen (eingeschränkten) Schutz zukommen lässt, überzeugt im Hinblick auf die Verbandssanktionsregeln des Art 63a Abs 3 ff BankG nicht. Bei verfassungs- und konventionskonformer Interpretation (ua am Massstab des Art 8 Abs 1 EMRK) geniessen richtigerweise auch **juristische Personen** – soweit ihnen im Einzelfall ein rechtswidriges Verhalten zugerechnet werden kann – den gesetzlich intendierten Schutz. Sie sind Adressaten von Strafnormen und gegebenenfalls Parteien eines Strafverfahrens. Schon daraus resultiert die Pflicht der FMA, auch die Identität von juristischen Personen – soweit geboten – geheim zu halten. Jede andere Auslegung wäre im Hinblick auf die Art 8 Abs 1 EMRK rechts-[58] bzw verfassungswidrig.[59]

Im Hinblick auf die von der FMA zu implementierenden **Schutzmechanismen** darf auf die Ausführungen zuvor verwiesen werden, die hier sinngemäss zugrunde zu legen sind.

IV. Anwendungsbereich des Hinweisgebersystems

Anders als österreichische Pendant des § 99g BWG[60] schränkt Art 64a Abs 1 BankG den **sachlichen Anwendungsbereich** des Hinweisgebersystems der FMA ein. Es umfasst neben Hinweisen auf (potentielle) **Verstösse gegen unmittelbar anwendbares EWR-Sekundärrecht** (**CRR**,[61] **MiFIR**[62]) den **Verdacht** eines Verstosses gegen das BankG und die BankV.[63]

Das Hinweisgebersystem gem BankG erfasst daher nicht auch Hinweise auf Verstösse gegen andere Landesgesetze, etwa das GewG,[64] das TVTG[65] etc. Da jedoch weder das LVG noch das FMAG das ein Beweisverwertungsverbot statuieren, ist die FMA dennoch grds berechtigt, einen ihr übermittelten Sachverhalt zu verwerten und einer weiteren Überprüfung zu unterziehen, daher ggfalls auch Verdachtsmomente nach anderen Gesetzen zu verarbeiten. Auch aus der DSGVO ergibt sich nichts Anderes.[66] Dafür spricht auch, dass die FMA – wie gezeigt – auch nach anderen Aufsichtsgesetzen ein externes Hinweisgebersystem einzurichten hat.

Das Hinweisgebersystem zielt darauf ab, extern eingemeldete Verdachtsmomente zu verarbeiten. Ein »**Verdacht**«, der nicht schwerwiegend oder konkret sein muss (arg »potentiell«), liegt bereits dann vor, wenn hinreichende Gründe vorliegen, welche die Annahme rechtfertigen, dass eine Person eine Rechtsverletzung iSd Art 64a Abs 1 BankG begangen haben könnte. Damit geht das Gesetz über den von der CRD IV gezogenen Rahmen hinaus, wonach Hinweisgebersysteme dro-

56 Dabei macht es aus Sicht der von der FMA zu vollziehenden Verwaltungsstrafbestimmungen keinen Unterschied, ob eine Person als unmittelbarer Täter oder als Bestimmungs- oder Beteiligungstäter gehandelt hat. Für die gerichtlich zu vollziehenden Strafbestimmungen gilt Ähnliches.

57 Gesetz vom 21. April 1922 über die allgemeine Landesverwaltungspflege (LVG), LGBl 1922.024.

58 Dass Art 71 Abs 2 CRD ebenfalls nur auf natürliche Personen abstellt, ändert nichts an der hier vertretenen Auffassung.

59 Zur Stellung der EMRK in Liechtenstein im Rang von Verfassungsrecht zuletzt eingehend *Schiess Rütimann*, Die Stellung der EMRK in Liechtenstein, Jusletter 4. Februar 2019 (zusammenfassend in Rz 184 ff).

60 Bankwesengesetz (BWG), ö BGBl 1993/532.

61 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012, ABl 2013 L 176, 1.

62 Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 Text von Bedeutung für den EWR, ABl 2013 L 173, 84.

63 Verordnung vom 22. Februar 1994 über die Banken und Wertpapierfirmen (Bankenverordnung), LGBl 1994,22.

64 Gewerbegesetz (GewG), LGBl 2006.184.

65 Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz; TVTG), LGBl 2019.301.

66 Zu bedenken ist, dass die FMA nach Art 22 Abs 1 FMAG ausdrücklich ermächtigt ist, auch Daten über strafrechtliche Verdachtsmomente zu verarbeiten. Zudem ergibt sich die entsprechende Befugnis der FMA aus Art 6 Abs 1 lit c; Art 10 DSGVO.

hende oder tatsächliche Verstösse gegen Aufsichtsrecht erfassen sollen (Art 71 Abs 2 leg cit).

Der **persönliche Anwendungsbereich** des Hinweisgebersystems ist ebenfalls weit gezogen. Es erfasst Verdachtsmomente, die einem aufsichtsunterworfenen Institut zugerechnet werden können. Art 64a Abs 3 BankG stellt idZ klar, dass eine (gutgläubige) Meldung durch Angestellte von Banken, Wertpapierfirmen und Finanzinstituten an die FMA ex lege nicht als Verstoss gegen eine vertragliche oder gesetzliche Geheimhaltungspflicht gilt und keine diesbezügliche Haftung der meldenden Person zur Folge haben darf.

Im Ergebnis bleibt anzumerken, dass der vom Gesetzgeber vorgesehene **Anwendungsbereich** für das Hinweisgebersystem der FMA **extensiv** ausgestaltet wurde. Art 64a BankG unterscheidet nicht nach der Schwere eines Verstosses; er ist daher auch Meldepflichtverletzungen und Fristversäumnisse anzuwenden.[67] Die CRD hätte jedoch Raum für eine »angepasste«, dh eingeschränktere und im Ergebnis sachlichere Umsetzung gelassen.

V. Institutsbezogenes Hinweisgebersystem

A. Allgemeines

Vom externen Meldesystem der FMA sind die internen Hinweisgebersysteme der liechtensteinischen Finanzintermediäre zu unterscheiden.

Banken und **Wertpapierfirmen** sind gem Art 22 Abs 2 Bst e BankG verpflichtet, ein »institutsbezogenes Hinweisgebersystem« einzurichten; andere Institute können ein solches System auf freiwilliger Basis implementieren.[68] Zweigstellen von EWR-Banken in Liechtenstein werden von Art 22 Abs 2 Bst e BankG nicht erfasst (ihre Pflicht zur Implementierung von Hinweisgebersystemen folgt aus dem Recht des Herkunftsstaates, etwa § 99g ö BWG[69]). Zweigstellen von Drittstaatsinstituten sind, da die selbst Bewilligungsträger sind, Regelungsadressat des Art 22 BankG.

Die genannten Institute haben dieses Hinweisgebersystem ihren **Mitarbeitenden** zugänglich zu machen; es sollte daher allen Mitarbeitern, zB durch Information im Intranet des Unternehmens, deutlich kommuniziert werden,

- wo das System eingerichtet ist,
- wie es erreicht werden kann und
- wie es funktioniert.

B. Einrichtung des Systems

Die Einrichtung und Organisation des Systems fällt in die Verantwortung der **Geschäftsleitung**.[70] Die Geschäftsleitung hat »**angemessene Verfahren**« zu implementieren, die Mitarbeitende in die Lage versetzen, Verstösse intern zu melden (dazu unten im Text); daher kann es geboten sein, Mitarbeitende des Instituts in der Handhabung des Systems zu schulen und ihnen die erforderlichen Hinweise über die Funktion des Systems zur Verfügung zu stellen etc.[71] Das Gesetz beschränkt sich, wie zumeist, darauf, Verhaltenspflichten der Geschäftsleitung zu statuieren, ohne nähere organisatorische Rahmenbedingungen festzulegen. Aus dem »Angemessenheitsprinzip« (wie es auch in Art 31 Abs 1 LV verankert ist) folgt, dass das System in Einklang mit Grösse, Risikogehalt der Geschäftstätigkeit und Komplexität der erbrachten Dienstleistungen des Instituts auszugestalten ist. Zur Auslegung des Terminus »Verfahren« s bereits oben im Text.

Die Geschäftsleitung hat daher sicherzustellen, dass es *für das* Institut (nicht notwendigerweise *im* Institut organisatorisch angesiedelt) ***ein*** »**Hinweisgebersystem**« gibt. Dieses System muss im Ergebnis geeignet sein, gemeldete Verstösse entgegenzunehmen. Die Stelle, welche das System betreibt, muss Hinweise auswerten können und über relevante Hinweise der Geschäftsleitung Bericht erstatten (Weiterverarbeitung von Hinweisen[72]). Daher muss nicht zwingend ein elektronisches System eingerichtet werden. Es genügt, wenn das System – etwa über eine telefonische »Hotline« – anonym Meldungen über Verstösse entgegennimmt. Soweit kompatibel, können auch bestehende Systeme als Hinweisgebersystem iSd Art 22 Abs 2 Bst e BankG verwendet werden.

67 Krit *Heidinger/Strauss* in *Gruber/N. Raschauer,* Whistleblowing 67; weiters *Majcen,* ÖBA 2014, 487 (489).

68 Oftmals kann sich für andere Institute eine Pflicht zur Einrichtung eines Hinweisgebersystems aus konzerninternen oder aus ausländischen Rechtsvorschriften ergeben.

69 *Lehner/Reisenberger* in *Dellinger,* BWG § 99g Rz 5.

70 Zur Ausgestaltung des Systems vgl auch *EBA*, Guidelines on Internal Governance (EBA-GL-2017-11) vom 26.9.2017 Rz 117 ff. Daraus ergibt sich zusammengefasst die Pflicht eines Instituts, entsprechende interne Warnmechanismen einzurichten, damit Mitarbeitende des Instituts Probleme in Verbindung mit der internen Governance melden können.

71 Eine Pflicht der Mitarbeitenden, das Hinweisgebersystem im Falle eines erkannten/vermuteten Verstosses auch tatsächlich zu nutzen, ist aus dem Gesetz nicht abzuleiten. Das Institut darf die Meldung aber jedenfalls nicht faktisch unmöglich machen, indem die Meldungslegung mit erheblichen Hürden versehen wird (zB durch hohe Kosten bei Meldung an eine Telefon-Hotline; *Lehner/Reisenberger* in *Dellinger,* BWG § 99g Rz 14).

72 *EBA*, Guidelines on Internal Governance Rz 120, hält in diesem Zusammenhang fest, dass die von den Mitarbeitenden im Rahmen dieses Verfahrens mitgeteilten Informationen, sofern sie sachdienlich sind, auch dem Leitungsorgan (ggfalls in anonymer Form) zur Kenntnis gebracht werden sollen.

Die Geschäftsleitung hat im Sinne der ratio legis *eine* »**geeignete Stelle**« einzurichten und mit dem Betrieb und der Organisation des Hinweisgebersystems zu betrauen. Diese Stelle muss nicht zwingend institutsintern eingerichtet sein, wenngleich sich aus Art 71 Abs 3 CRD IV iVm Art 22 Abs 2 Bst e BankG eine deutliche »Präferenz« des (EWR-)Gesetzgebers für eine »interne Lösung« ableiten lässt. Die geeignete Stelle kann beispielweise auch in einer übergeordneten Bank angesiedelt werden.

Es ist ferner zulässig, die angesprochene Aufgabe auch durch einen fachlich geeigneten **externen (Compliance)Dienstleister** (zB WP, RA und dergleichen) auf vertraglicher Basis wahrzunehmen zu lassen, wobei diesfalls in einem Vertrag adäquate Regelungen zum Berichtsprozess, über einen Reaktionsplan im Fall einer Meldung, zur Geheimhaltung etc festzuhalten sind (s auch Art 28 Abs 3 DSGVO). Unter Umständen sind auch **Kombinationslösungen** denkbar, wobei diesfalls (aus Sicht der FMA) an der Effektivität des Systems zu zweifeln sein könnte. Auch eine solche Meldung an eine externe Stelle gilt – gemessen an Art 71 Abs 3 UAbs 2 CRD IV – als »interne Meldung«, weil die extern beauftragte Stelle das Institutssystem im Auftrag der Geschäftsleitung des Instituts betreibt, an die Geschäftsleitung berichtet und das System Mitarbeitenden des Instituts offen steht.[73]

Entscheidet sich die Geschäftsleitung, das Hinweisgebersystem bei einer **institutsinternen Stelle** zu implementieren, ist sicherzustellen, dass die Stelle nicht innerhalb der üblichen Stab-Linien-Organisation des Instituts angesiedelt wird; nach Art 71 Abs 3 CRD IV iVm Art 22 Abs 2 Bst e BankG ist ein »**spezieller Kanal**« einzurichten. Die Stelle soll nach den Vorstellungen des EWR-Gesetzgebers und der EBA »ausserhalb der regelmässigen Berichtswege« eingerichtet sein.[74] Naheliegend ist es daher, das Hinweisgebersystem bei der Compliance-Stelle, der Innenrevision oder bei einer speziellen Stabstelle (»Ombudsmann«) anzusiedeln, die direkt der Geschäftsleitung unterstellt und gegebenenfalls direkt bei der Geschäftsleitung eingerichtet ist (Verkürzung der dienstlichen Berichtswege). Es schadet im Ergebnis nicht, wenn die betraute Stelle bereits andere Aufgaben wahrnimmt. Um Interessenkonflikte zu vermeiden, sollte jedoch gewährleistet sein, dass die jeweiligen Aufgaben miteinander »kompatibel« sind.

C. Organisatorische Rahmenbedingungen für das institutsbezogene Hinweisgebersystem

Art 71 Abs 3 CRD IV verlangt, dass die spezielle Stelle, bei der das Hinweisgebersystem eingerichtet ist, **unabhängig** und **autonom** agieren kann.[75],[76]

Mit »**Unabhängigkeit**« ist gemeint, dass die Stelle, die das System betreibt, aufgabenbezogen frei von internen und externen Weisungen, frei von äusseren Einflüssen und ausserhalb der üblichen Berichtswege agieren können muss; welche Berichte als sachdienlich bewertet werden und welche Hinweise in welcher Form an die Geschäftsleitung weiterzuleiten sind, entscheidet zunächst die beauftragte Stelle. In diesem Zusammenhang ist es zulässig, wenn die Geschäftsleitung bestimmte Richtlinien für den Berichts- und Reaktionsprozess vorgibt, etwa, in welcher Form bzw binnen welcher Frist Berichte zu erstatten sind. Nur dann, wenn die beauftragte Stelle unabhängig agieren kann, kann das Hinweisgebersystem bei der Aufdeckung gravierender Compliance-Verstösse helfen und zur Schadensminimierung im Institut beitragen. Nur dann können mögliche Schwachstellen in den Prozessen des Instituts aufgedeckt und geeignete Reaktionsmöglichkeiten erörtert werden.[77]

Mit »**Autonomie**« soll im Zusammenhang mit der Unabhängigkeit der Stelle zum Ausdruck gebracht werden, dass die Stelle das Hinweisgebersystem eigenständig, selbstbestimmt und gleichberechtigt (dh effektiv) neben anderen Aufgaben, die dieser Stelle übertragen sind, betreiben können soll. Dies setzt etwa voraus, dass der Stelle, wenn ihr auch andere Aufgaben zukommen sollen, nur solche Agenden zugewiesen werden dürfen, die mit dem Hinweisgebersystem kompatibel sind; **Interessenkonflikte** sind zu vermeiden. Zudem bedingt Unabhängigkeit und Autonomie, dass die Stelle – wenn sie unternehmensintern besetzt wird – über eine adäquate Personal-, Budget- und Sachausstattung verfügt. Bei externen Stellen hat die beauftragende Geschäftsleitung darauf hinzuwirken, dass eine geeignete Stelle beauftragt wird, die von ihrer Ausstattung und Organisation her in der Lage ist, den Auftrag zu erfüllen.

Das Institut hat das Hinweisgebersystem derart einzurichten und zu organisieren, dass durch »**angemessene Verfahren**« betriebsinterne Verstösse gemeldet,[78]

73 Für diese Auffassung spricht, dass Art 71 Abs 3 UAbs 2 CRD IV explizit die Heranziehung eines externen Systembetreibers erlaubt (arg »Sozialpartner«).

74 *EBA,* Guidelines on Internal Governance Rz 117; s auch ErläutRV 2438 BlgNR 24. GP 64.

75 Arg »unabhängiger und autonomer Kanal«.

76 Die Unabhängigkeit des Systems wird auch in *EBA,* Guidelines on Internal Governance Rz 117, betont. Vgl auch aaO Rz 118 zur institutsinternen Umsetzung.

77 Vgl auch *Prebil/Schäfer,* Der Einsatz von Hinweisgebersystemen in Banken, Compliance Praxis H 4/2013, 6.

78 *Lehner/Reisenberger* in *Dellinger,* BWG § 99g Rz 8 weisen darauf hin, dass das Gesetz nur das Meldeverfahren, nicht jedoch das Auswertungs- bzw Untersuchungsverfahren regle. Es bleibe daher dem Institut überlassen, wie die »geeignete Stelle« mit

ausgewertet und effektiv untersucht werden können. Folgende Verfahrensschritte könnten zu implementieren und im Verdachtsfall zu setzen sein:[79]

- Klärung über Art und Dimensionierung des Hinweisgebersystems;
- Eindeutige und klare Definition der Meldekategorien;
- Implementierung des Systems;
- Einholen relevanter Zustimmungen/Einwilligungen (etwa der Mitarbeitenden, des Verwaltungsrates etc);
- Etablieren eines Prozesses zum Umgang mit Fällen aus dem Hinweisgebersystem (Richtlinien; Berichtswesen);
- Etablierung eines Untersuchungsteams innerhalb der »zuständigen Stelle« (Vier-Augen-Prinzip);
- vertrauliche Überprüfung von Hinweisen;
- Überprüfung der rechtlichen Auswirkungen des Falles;
- Überprüfung des vom Fall ausgehenden Risikos (finanzielles Risiko und Reputationsrisiko);
- vertrauliche Einbindung des verantwortlichen Vorgesetzten des Verdächtigen;
- Überprüfung des Geschäftsprozesses;
- In der Folge legen zuständige Stelle und Compliance Officer die einzuleitenden Resolutionen fest;
- Bericht an die Geschäftsleitung und/oder den Verwaltungsrat;
- Festlegung von Reaktionsmassnahmen (zB Freistellung der Mitarbeitenden, Beweissicherung, Sperren von Zugangsrechten);
- Anpassung von Geschäftsprozessen;
- Entscheidung über allfällige externe Berichterstattung und Massnahmen wie Verdachtsmeldungen, Strafanzeige, Information an Dritte;
- Protokollierung der gesetzten Schritte.

D. Weitere Kriterien

Das Hinweisgebersystem muss den in Art 71 Abs 2 CRD IV definierten Kriterien entsprechen (diese wurden im Gesetz nicht explizit umgesetzt; s jedoch § 99g Abs 3 ö BWG und dazu schon oben im Text). Das BankG ist jedoch einer richtlinienkonformen (bzw gemessen an Art 8 Abs 1 EMRK, einer konventionskonformen) Auslegung zugänglich. Daraus folgt, dass es

- einen **angemessenen Schutz für Mitarbeitenden** von Instituten bieten muss. Dies ist dann gewährleistet, wenn die Anonymität des Hinweisgebers während des gesamten internen Ermittlungsverfahrens gegenüber Dritten (zB anderen Mitarbeitenden) gewährleistet ist; Dritten gegenüber dürfen daher insb keine personenbezogenen Daten über den Hinweisgeber offengelegt werden. Dadurch soll der Hinweisgeber vor Vergeltungsmassnahmen, Diskriminierung oder anderen Arten von Mobbing geschützt werden. Das Hinweisgebersystem ist daher auch technisch derart zu gestalten, dass die Identität des Hinweisgebersystems für Dritte mit legalen Mitteln nicht ermittelt werden kann (Sicherstellung der Geheimhaltung); vice versa muss die Stelle, die mit dem Betrieb des Hinweisgebersystems beauftragt ist, einer **strikten Geheimhaltungspflicht** unterworfen sein (vgl etwa Art 28 Abs 3 Bst b DSGVO). Zudem ist in den Richtlinien der Geschäftsleitung sicherzustellen, dass der Berichtsprozess an die Geschäftsleitung derart abgewickelt wird, dass die Identität des Hinweisgebers grundsätzlich nicht offengelegt wird.
- Wie bereits zuvor ausgeführt, verlangen weder Art 8 Abs 1 EMRK, die CRD IV noch das BankG (im Zusammenhang mit Hinweissystemen der FMA) einen absoluten Schutz der Identität des Hinweisgebers; nichts Anderes wird daher in einem Grössenschluss auch für interne Hinweisgebersysteme von Banken und Wertpapierfirmen zu vertreten sein. Das Institut ist berechtigt, personenbezogene Daten über den Hinweisgeber zu speichern und zu verarbeiten, wenn der Stelle diese Daten gegenüber freiwillig offengelegt werden (zB Name, Funktion, Adresse des Hinweisgebers und dergleichen).[80] Das Institut ist ferner ermächtigt, die Daten des Hinweisgebers an Dritte weiterzugeben, soweit dies der Hinweisgeber ausdrücklich legitimiert bzw soweit dies gesetzlich vorgesehen und im Anlassfall, etwa für die Einvernahme als Zeuge in einem gerichtlichen Strafverfahren, unbedingt erforderlich ist.
- einen **adäquaten Schutz personenbezogener Daten** des Hinweisgebers als auch des Tatverdächtigen gewährleistet: Wie bereits zuvor ausgeführt, muss ein elektronisches System technisch ausgereift sein, dh dem Stand der Technik entsprechen; es müssen adäquate Datensicherheitsmassnahmen implementiert werden (Art 24 ff; 32 DSGVO), Vertraulichkeitsbereiche und klare Zugriffsrechte vorgesehen werden; ferner muss unternehmensintern angeordnet und kontrolliert werden, dass die Mitarbeitenden der »zuständige Stelle« der Verschwiegenheitspflicht unterliegen (Art 14 BankG). Das Institut hat

den erhaltenen Meldungen weiter verfährt. Es ist jedoch unbestreitbar, dass auch das Auswertungsverfahren in angemessener Weise ausgestaltet werden muss, um den Schutz sowohl des Hinweisgebers als auch des Beschuldigten zu gewährleisten.

79 Vgl *Prebil/Schäfer,* Compliance Praxis H 4/2013, 6.

80 Es besteht daher kein gesetzliches Verwertungsverbot.

in einem »internen Verhaltenskodex« festzulegen, welche Mitarbeitenden des Instituts unter welchen Voraussetzungen Zugriff auf das System und die in weiterer Folge gespeicherten Daten und Informationen erhalten. Es ist ferner klarzustellen, für welche Zwecke Daten verwendet werden dürfen. Der Zugriff auf die Daten wie auch die weitere Verwendung ist zu protokollieren und dergleichen.

- unternehmensintern klare **Regeln** geben muss, welche die **Geheimhaltung der Identität** der Person, die die Verstösse anzeigt, **gewährleisten**: In Richtlinien der Geschäftsleitung, die gemeinsam mit der »zuständigen Stelle« (welche das Hinweisgebersystem betreibt) entwickelt werden, ist einerseits klarzustellen, dass die Geheimhaltungspflicht für das Institut und die zuständigen Mitarbeitenden der Stelle gilt, wenn der Hinweisgeber selbst seine Identität offenlegt, andererseits aber auch dann, wenn die Identität des Hinweisgebers zufällig (etwa aufgrund einer Unachtsamkeit des Hinweisgebers selbst) oder im Zuge der weiteren Untersuchung bekannt wird. In diesem Zusammenhang ist in den Richtlinien auch klarzustellen, wann und wem gegenüber eine Offenlegung der Identität des Hinweisgebers erfolgen darf. Auch hier zeigt sich, dass der Schutz des Hinweisgebers nicht absolut gewährleistet ist; mitunter kann es erforderlich sein, seine Identität gegenüber Strafverfolgungsbehörden offenzulegen (um ihn als Zeuge einvernehmen zu können etc).

E. Anwendungsbereich des institutsbezogenen Hinweisgebersystems

Anders als § 99g Abs 1 ö BWG zieht das BankG (Art 22 Abs 2 Bste e) den **sachlichen Anwendungsbereich** des institutsbezogenen Hinweisgebersystems nicht weit. Anders als die ö Pendantnorm erfasst das BankG nur die CRR und das BankG als Beurteilungsrahmen, nicht aber sonstige Regelungen.[81] Unklar ist, warum in der Auflistung die BankV nicht genannt wurden. Auch Verfügungen, Mitteilungen der FMA etc fehlen im Text.

Das institutsinterne Hinweisgebersystem ist nicht auf »**betriebsinterne** (bzw konzerninterne) **Verstösse**« beschränkt. Auch Verstösse, die sich bei einem externen Vertragspartner (Outsourcingpartner) des Instituts, bei einer Tochtergesellschaft etc ereignen, können unter Art 22 Abs 2 Bst e BankG subsumiert werden.

Erfasst sind jedenfalls betriebsinterne Verstösse. Das sind Verstösse von **Mitarbeitenden, die einem Institut zugerechnet werden können** und welche in Ausübung einer betrieblichen Funktion, also in der Tätigkeit für bzw in Vertretung eines Instituts begangen werden.[82]

Gegenstand der Meldung kann nicht nur ein tatsächlicher Verstoss gegen die in Art 22 Abs 2 Bst e BankG abschliessend aufgezählten Vorschriften sein, sondern – bei richtlinienkonformer Auslegung am Massstab des Art 71 CRD – auch jeder **Verdacht** eines solchen Verstosses (es handelt sich um einen »potentiellen Verstoss«, vgl auch Art 64a BankG).

Davon sind wiederum Verstösse gegen andere unternehmensinterne Anweisungen, Richtlinien und dergleichen zu unterscheiden. Selbstverständlich ist es zulässig, wenn ein Institut beschliesst, sein Hinweisgebersystem auf solche Verstösse zu erweitern. Letzteres ist jedoch nicht mehr Regelungsgegenstand des Art 22 Abs 2 Bst e BankG.

Was den **persönlichen Anwendungsbereich** des institutsbezogenen Hinweisgebersystems betrifft, sind zwei Aspekte zu unterscheiden:

- Es ist allen **aktiven Mitarbeitenden** des Instituts (als potenziellen Hinweisgebern) sowie gegebenenfalls auch vertraglich gebundenen Dienstleistern zugänglich zu machen;[83] auf Basis welcher Rechtsgrundlage der Mitarbeitende beim Institut beschäftigt ist, spielt dabei keine Rolle. Das Gesetz erfasst daher auch Leiharbeitskräfte, werkvertraglich für das Institut tätige Personen (man denke an Outsourcing-Kooperationspartner), Mandatare in Gremien und Organe, durch Entsendungen oder sonst etwa im Konzern aufgrund bestimmter Leistungsvereinbarungen funktional für das Institut tätige Personen.[84] Bereits seit längerem ausgeschiedene und pensionierte (daher »ehemalige«) Mitarbeiter sind wohl nicht unmittelbar Zielgruppe des internen Hinweisgebersystems; freilich folgt daraus nicht, dass das Hinweisgebersystem keine Hinweise von ehemaligen Mitarbeitenden des Instituts (mehr) entgegennehmen dürfte. Wenn jene daher Zugang zum Hinweisgebersystem besitzen, erscheint es nicht ausgeschlossen, dass auch diese Personen Hinweise übermitteln, wenn sie Kenntnis über einen betriebsinternen Verstoss haben.
- Davon sind jene **Mitarbeiter** zu unterscheiden, die einer Rechtsverletzung **verdächtigt** werden. Der durch das Institut zu gewährleistende Schutz kommt angezeigten Mitarbeitenden nur insoweit zugute, als sie in jenem Zeitraum, auf den sich eine Meldung bezieht, beim Institut beschäftigt waren und mut-

81 Vgl aber Art 71 der RL, der ausdrücklich auf die nationalen Umsetzungsvorschriften zur RL Bezug nimmt.

82 *Lehner/Reisenberger* in *Dellinger,* BWG § 99g Rz 16.

83 *EBA,* Guidelines on Internal Governance Rz 119.

84 *Lehner/Reisenberger* in *Dellinger,* BWG § 99g Rz 10.

masslich für einen Verstoss verantwortlich sind.[85] Zur Beschäftigungsgrundlage gilt das zuvor Gesagte sinngemäss.

VI. Grundrechtliche Implikationen

Die Verletzung gesetzlich oder vertraglich auferlegter Verschwiegenheitspflichten durch einen Geheimnisträger, soweit dies durch eine Anzeige mittels Hinweisgebersystems erfolgt, kann in vielen Fällen rechtswidrig sein (vgl § 1328a ABGB; § 1173a Art 4 Abs 4 ABGB; Art 82 f DSGVO; §§ 121 f StGB; Art 83 DSGVO ua). Doch ist der Whistleblower tatsächlich in jedem Einzelfall zu bestrafen? Nein. So bestimmt schon § 122 Abs 4 StGB, dass die Offenbarung von Geheimnissen mitunter im öffentlichen oder privaten Interesse gerechtfertigt sein kann.

Auch der EGMR[86] hat in seiner stRsp zu Art 10 Abs 1 EMRK wiederholt festgehalten, dass eine Anzeige/Meldung und damit die Offenbarung von Geheimnissen durch die **Meinungsfreiheit** geschützt sind, wenn die Anzeige als ultima ratio erfolgt, um auf einen Missstand (etwa im Unternehmen) aufmerksam zu machen. Eine Rechtfertigung erfolgt jedoch nur, wenn es aus der Perspektive des Meldungslegers keine anderen effektiven Mittel zur Abstellung des Missstandes gibt, womit etwa der Hinweis an eine vorgesetzte Stelle angesprochen ist. Bemerkenswert ist in diesem Zusammenhang, dass nach Auffassung des EGMR Whistleblowing jedenfalls als ultima ratio geschützt sein müsse. Das bedeutet letzten Endes, dass sich ein Informant, der gegen rechtlich anerkannte Geheimhaltungspflichten verstossen hat, uU auf sein Grundrecht der Meinungsfreiheit berufen kann; das Interesse eines Unternehmens bzw der Öffentlichkeit an der Aufdeckung fragwürdiger (hier: unternehmensinterner) Vorgänge kann daher bei einer entsprechenden Interessenabwägung im Einzelfall das Interesse des Arbeitgebers oder des Staates an Geheimhaltung überwiegen. Freilich ist die angesprochene Judikatur kein Freibrief für Denunzianten und investigative Journalisten: Die externe Weitergabe heikler Daten sollte erst erfolgen, wenn kein anderer gleich effektiver Weg besteht, um Missstände organisationsintern abzustellen. Dieser Auffassung hat sich der StGH rezent in seinem Urteil 2018/074 angeschlossen.

VII. Resümee und Ausblick

Ein funktionsfähiges Hinweisgebersystem gehört mittlerweile, wie gezeigt wurde, zur »Standardeinrichtung« einer funktionsfähigen Governance in öffentlichen Unternehmen wie der FMA sowie in Banken und Wertpapierfirmen.

Am Horizont der EU-Rechtslandschaft zeigt sich in Gestalt der »Whistleblowing-RL« (EU) 2019/1937,[87] dass zukünftig auch in anderen Wirtschaftsbereichen Unternehmen Hinweisgebersysteme einrichten werden müssen. Bis zur Umsetzung der Richtlinie auf EU-Ebene wird noch etwas Zeit vergehen. Ob und inwieweit die RL in das EWR-Abkommen übernommen wird, ist ebenso unklar.

Allerdings kann am Ende festgehalten werden, dass eine gute Corporate Governance in einem Unternehmen (nicht nur in der Finanzbranche) ohne Hinweisgebersystem langfristig nicht auskommen kann. Argumentative Versuche, Hinweisgebersysteme als Verstoss gegen ordre-public-Grundsätze[88] oder als »organisiertes Denunziantentum« abzutun,[89] gehören seit Inkrafttreten der Whistleblowing-RL der Vergangenheit an.

Korrespondenz:
Prof. Dr. Nicolas Raschauer,
Inhaber des Propter Homines Lehrstuhls
für Bank- und Finanzmarktrecht,
Leiter des Instituts für Wirtschaftsrecht,
Universität Liechtenstein,
Fürst Franz Josef-Strasse, 9490 Vaduz,
T 423 265 11 11,
Mail: finanzmarktrecht@uni.li.

85 Dabei kommt nicht nur unmittelbare Täterschaft, sondern auch Bestimmungs- und Beitragstäterschaft in Betracht.

86 Zur Thematik zB *Pabel,* Der grundrechtliche Schutz des Whistleblowing in FS Berka 161; *Dworschak/N. Raschauer*, Whistleblowing in Druck. Siehe weiterführend StGH 2018/074 (betreffend arbeitsrechtlichen Schutz eines anzeigenden Arztes), der auf die aktuelle EGMR-Rsp Bezug nimmt; EGMR *Guja* (appl 14.277/04, 2008): Verrat von Amtsgeheimnissen in Moldawien im Vorfeld von Parlamentswahlen; EGMR *Heinisch* (appl 28.274/08, 2011): Strafanzeige gegen Vivantes wegen des Verdachts auf Betrug (Personal- und Qualitätsmängel in der Pflege); EGMR *Bargao* (appl 53.579/09 ua, 2012): Verwaltungsassistent wies auf Verfehlungen in einem öffentlichen Gesundheitszentrum hin; EGMR *Bucur* (appl 40.238/02, 2013): Mitarbeiter des rumänischen Geheimdienstes decken in einer Pressekonferenz bestehende Praxis illegaler Abhöraktionen und das Fehlverhalten ihrer Vorgesetzten auf.

87 Die angesprochene RL wurde erst am 26.11.2019 im Amtsblatt der Europäischen Union verlautbart. Die EU-Mitgliedstaaten haben diese bis 17.12.2021 umzusetzen. Es ist wahrscheinlich, dass Liechtenstein die RL wegen der politischen und wirtschaftlichen Bedeutung vorab in nationales Recht umsetzen wird, sollte die RL bis 2021 nicht in das EWRA übernommen worden sein. Für den EWR entfaltet die RL (bislang) keine Rechtswirkung, seine Übernahme in das EWR-Abkommen steht derzeit auf dem Prüfstand: <https://www.efta.int/eea-lex/32019L1937> (abgerufen am 18.5.2020).

88 Siehe dazu (bezogen auf Amtshilfe in Steuersachen) StGH 2019/027.

89 Vgl die Diskussion bei *Dworschak/N. Raschauer*, Whistleblowing.