

Die «Whistleblowing-Richtlinie» der Europäischen Union und deren Auswirkungen auf die Unternehmenspraxis

17. Dezember 2021

Gutachten

der

Zürcher Hochschule für angewandte Wissenschaften (ZHAW)

Zentrum für Wettbewerbsrecht und Compliance (ZWC)

zuhanden

TELAG AG

Hardturmstrasse 101
8005 Zürich
Schweiz

Snubes GmbH

Prinzessinnenstrasse 19/20
10969 Berlin
Deutschland

Gutachter

Prof. Dr. Patrick Krauskopf, Leitung ZWC, ZHAW

Dr. Katharina Britta Hastenrath, Studienleitung, ZHAW

Armin Flavius Dugan, MLaw, Wissenschaftlicher Mitarbeiter, ZHAW

Projektmitarbeitende

Ceren Bingöl, BLaw, ZHAW

I. Executive Summary (D / FR / IT)

Hintergrund. Durch die 2019 in Kraft getretene EU-Richtlinie 2019/1937 sollen Mindeststandards für Hinweisgeber (sog. «Whistleblower») eingeführt werden. Sofern Whistleblower künftig Rechtsverstöße am Arbeitsplatz offenlegen wollen, sollen sie die Meldung hierzu unbeirrt und mittels eines vertraulichen Meldesystems vornehmen können – gerade ohne Repressalien des Arbeitgebers fürchten zu müssen.

Die Mitgliedsstaaten haben noch bis zum Stichtag 17.12.2021 Zeit, die Richtlinie in nationales Recht umzusetzen. Die Richtlinie betrifft Unternehmen, sofern sie einer Geschäftstätigkeit in der EU nachgehen und am jeweiligen Standort mindestens 50 Mitarbeiter beschäftigt sind.

Auftrag. Die ZHAW ist durch die TELAG AG und Snubes GmbH beauftragt worden, zu analysieren, welche Auswirkungen die Richtlinie aus unternehmerischer Perspektive für den Bereich Compliance und das Unternehmen hat.

Empirische Untersuchung. Zur Beantwortung der Forschungsfrage wurde im Zeitraum vom 16.11.2021 bis 30.11.2021 mittels eines Fragebogens eine anonyme Umfrage unter knapp 8'000 Unternehmen aus der DACH-Region, welche in unterschiedlichsten Branchen tätig sind, durchgeführt. Die Adressaten wurden per E-Mail kontaktiert und um die Teilnahme an der Umfrage gebeten.

Inhaltlich wurden neben den soziodemografischen Merkmalen der Unternehmen (Anzahl Mitarbeitende, geografische Aktivitäten), letztere auch nach Motiven für die Einführung eines Meldesystems befragt und ob sie ein solches System bereits implementiert haben oder dies zukünftig vorhaben. Die Befragten wurden um Angaben zu den wünschenswerten Eigenschaften eines Meldesystems gebeten, sowie dazu, ob sie ein internes oder aber ein externes System eines Drittanbieters bevorzugen.

1. Befund: Motive. Unternehmensinterne Motive, wie bspw. eine transparente Unternehmenskultur, sind für die Einführung eines Meldesystems genauso relevant wie eine gesetzliche Pflicht.

2. Befund: Meldekanäle. Die E-Mail wird von Unternehmen mit signifikantem Abstand als wichtigster Meldekanal für Whistleblower angegeben. Ein statistischer Zusammenhang zwischen den Eigenschaften eines Meldesystems (Kosten, Einfachheit der Prozesseinbettung und Anonymität des Hinweisgebers) und den bevorzugten Meldekanälen (Telefon, Internet, Ombudsstelle, etc.) der Unternehmen lässt sich nicht ableiten.

3. Befund: Intern vs. Extern. In Bezug auf die Kosten und die Einfachheit eines Meldesystems zeigen Unternehmen keine Präferenz hinsichtlich interner oder externer

Meldesysteme. In Bezug auf die Anonymität des Hinweisgebers hingegen schon: Es werden eindeutig auswärtige Systeme von Drittanbietern bevorzugt. Bezüglich des gewünschten Serviceniveaus (24h-Erreichbarkeit, kurze Reaktionszeiten, Lösungen und Empfehlungen, etc.) sind die Unternehmen in der Wahl intern vs. extern indifferent. Lediglich ein mehrsprachiger Service korreliert mit der Entscheidung für ein externes Hinweisgebermeldesystem.

4. Befund: Unternehmensgrösse. Grosse Unternehmen (ab 250 Mitarbeitende) sind bezüglich einer Meldestelle weniger kostensensibel. Eine spezifische Vorliebe für externe Meldesysteme lässt sich bei ihnen nicht beobachten. Zudem haben Grossunternehmen mit einer höheren Wahrscheinlichkeit Hinweisgebersysteme bereits implementiert.

5. Befund: Schweizer Unternehmen. In Relation zu den anderen Unternehmen in der Stichprobe haben Schweizer Unternehmen teilweise andere Ansprüche an das Serviceniveau und die bevorzugten Meldekanäle eines Whistleblowersystems: Sie verleihen Ombudsstellen mehr Gewicht und legen weniger Wert auf die DSGVO-Konformität. Da sie gesetzlich nicht dazu verpflichtet sind, planen Schweizer Unternehmen die Einführung von Hinweisgebersystemen erst 2025 oder später ein – eindeutig später als solche aus der EU. Schweizer Unternehmen unterscheiden sich in ihrer Präferenz zu internen oder externen Meldesystemen nicht von denjenigen in den übrigen Ländern.

Contexte. La directive européenne 2019/1937, qui est entrée en vigueur en 2019, vise à introduire des normes minimales pour les lanceurs d'alerte. Si les lanceurs d'alerte souhaitent à l'avenir révéler des violations du droit sur le lieu de travail, ils doivent pouvoir le faire sans crainte et au moyen d'un système de signalement confidentiel - précisément sans devoir craindre des représailles de la part de l'employeur.

Les États membres ont jusqu'au 17 décembre 2021 pour transposer la directive dans leur droit national. La directive concerne les entreprises qui exercent une activité commerciale dans l'UE et qui emploient au moins 50 personnes sur leur site.

Charge. La ZHAW a été chargée par TELAG AG et Snubes GmbH d'analyser les conséquences de la directive dans une perspective entrepreneuriale pour le domaine de la conformité et l'entreprise.

Enquête empirique. Pour répondre à la question de recherche, une enquête anonyme a été menée entre le 16.11.2021 et le 30.11.2021, au moyen d'un questionnaire, auprès de près de 8'000 entreprises de la région DACH, actives dans les secteurs les plus divers. Les destinataires ont été contactés par e-mail et priés de participer à l'enquête.

Outre les caractéristiques sociodémographiques (nombre de collaborateurs, activités géographiques) des entreprises, ces dernières ont également été interrogées sur les motifs d'introduction d'un système de déclaration et sur le fait de savoir si elles avaient déjà mis en place un tel système ou si elles prévoyaient de le faire dans l'avenir. Les répondants ont été invités à indiquer les caractéristiques souhaitables d'un système de signalement et s'ils préféreraient un système interne ou externe d'un fournisseur tiers.

1^{er} constatation: les motivations. Les motifs internes à l'entreprise, comme par exemple une culture d'entreprise transparente, sont tout aussi importants pour l'introduction d'un système de signalement qu'une obligation légale.

2^{ième} constatation: les canaux. Le courrier électronique est cité par les entreprises comme le principal canal de signalement des lanceurs d'alerte, avec une distance significative. Il n'est pas possible d'établir un lien statistique entre les caractéristiques d'un système de signalement (coût, simplicité d'intégration du processus et anonymat du lanceur d'alerte) et les canaux de signalement préférés des entreprises (téléphone, Internet, service de médiation, etc.).

3^{ième} constatation: interne vs. externe. En ce qui concerne les coûts et la simplicité d'un système de signalement, les entreprises ne montrent aucune préférence pour les systèmes de signalement internes ou externes. En revanche, elles le font en ce qui concerne l'anonymat du lanceur d'alerte : elles préfèrent clairement les systèmes externes de

fournisseurs tiers. En ce qui concerne le niveau de service souhaité (joignabilité 24h/24, temps de réaction courts, solutions et recommandations, etc.), les entreprises sont indifférentes dans le choix interne vs externe. Seul un service multilingue est en corrélation avec le choix d'un système de signalement externe.

4^{ième} constatation: la taille de l'entreprise. Les grandes entreprises (à partir de 250 collaborateurs) sont moins sensibles aux coûts systèmes de signalement. On n'observe pas chez elles de préférence spécifique pour les systèmes de signalement externes. En outre, les grandes entreprises plus probablement ont déjà mis en place des systèmes de signalement.

5^{ième} constatation : entreprises suisse. Par rapport aux autres entreprises de l'échantillon d'analyse de l'enquête, les entreprises suisses ont des besoins partiellement différents en ce qui concerne le niveau de service et les canaux de signalement préférés d'un système de dénonciation: elles apprécient davantage les services de médiation et accordent moins d'importance à la conformité au RGPD. Comme elles n'y sont pas légalement tenues, les entreprises suisses ne prévoient d'introduire des systèmes de dénonciation qu'en 2025 ou plus tard - clairement plus tard que celles de l'UE. Les entreprises suisses ne se distinguent pas de celles des autres pays dans leur préférence pour les systèmes de signalement internes ou externes.

Contesto. La direttiva UE 2019/1937, entrata in vigore nel 2019, mira ad introdurre standard minimi per gli informatori (detti « whistleblower »). Se in futuro whistleblower vorranno rivelare violazioni legali sul posto di lavoro, dovranno avere la possibilità di farlo imperturbabili e per mezzo di un sistema di segnalazione confidenziale – senza dover temere rappresaglie da parte del datore di lavoro.

Gli Stati membri hanno tempo fino al 17. Dicembre 2021 per trasporre la direttiva nel diritto nazionale. La direttiva si applica alle aziende che commerciano nell'UE e hanno almeno 50 dipendenti nella rispettiva sede.

Incarico. La ZHAW è stata incaricata da TELAG AG e Snubes GmbH di analizzare l'impatto che la direttiva avrà sul settore della conformità e sull'azienda dal punto di vista imprenditoriale.

Analisi empirica. Per rispondere alla domanda della ricerca, dal 16.11.2021 al 30.11.2021 è stato condotto un sondaggio anonimo per mezzo di un questionario tra quasi 8'000 aziende nella regione DACH - attive in una vasta gamma di settori. I destinatari sono stati contattati via e-mail ed invitati a partecipare al sondaggio.

Oltre alle caratteristiche socio-demografiche (numero di dipendenti, attività geografiche) delle aziende, a queste ultime sono state chieste anche le motivazioni per l'introduzione di un sistema di reporting e se avessero già implementato un tale sistema o prevedessero di farlo in futuro. Agli intervistati è stato chiesto quali sono le caratteristiche desiderabili di un sistema di reporting e se preferissero un sistema interno o uno esterno di terzi.

1a constatazione: motivi. I motivi interni, ad esempio una cultura aziendale trasparente, sono altrettanto rilevanti per l'introduzione di un sistema di reporting quanto un obbligo legale.

2a constatazione: canali di segnalazione. Le aziende citano, con un margine significativo, l'e-mail come il canale di segnalazione più importante per i whistleblower. Non è possibile dedurre una correlazione statistica tra le caratteristiche di un sistema di segnalazione (costi, semplicità di integrazione del processo e anonimato del whistleblower) e i canali di segnalazione preferiti (telefono, internet, ufficio del difensore civico, ecc.) dalle aziende.

3a constatazione: interno vs. esterno. In termini di costi e di semplicità di un sistema di reporting, le aziende non mostrano alcuna preferenza tra i sistemi di reporting interni o esterni. Per quanto riguarda l'anonimato del whistleblower invece sì: i sistemi esterni di fornitori terzi vengono chiaramente preferiti. In merito al livello di servizio desiderato (disponibilità 24 ore su 24, tempi di risposta brevi, soluzioni e raccomandazioni, ecc.), le

aziende sono indifferenti nella scelta tra interno ed esterno. Solo un servizio multilingue è correlato alla decisione di un sistema di segnalazione esterno degli informatori.

4a constatazione: dimensione dell'azienda Le grandi aziende (250 dipendenti o più) sono meno sensibili ai costi in merito ad un sistema di segnalazione. Tra di loro non si mostra nessuna preferenza specifica per sistemi di reporting esterni. Inoltre è più probabile che le grandi aziende abbiano già implementato sistemi di whistleblowing.

5a constatazione: aziende svizzere. Rispetto alle altre aziende del campione d'analisi del sondaggio, le aziende svizzere hanno esigenze parzialmente diverse riguardanti il livello di servizio e i canali di segnalazione preferiti di un sistema per informatori: danno più valore ai servizi del difensore civico e danno meno importanza alla conformità al GDPR. Non essendo legalmente obbligate a farlo, le aziende svizzere non prevedono di implementare sistemi di whistleblowing prima del 2025 o addirittura più tardi – nettamente in ritardo rispetto di quelle dell'UE. Le aziende svizzere non differiscono nella loro preferenza per i sistemi di reporting interni o esterni da quelle degli altri paesi.

II. Inhaltsverzeichnis

| | | |
|-------|---|------|
| I. | EXECUTIVE SUMMARY (D / FR / IT) | I |
| II. | INHALTSVERZEICHNIS..... | VII |
| III. | LITERATURVERZEICHNIS | VIII |
| IV. | MATERIALIENVERZEICHNIS | IX |
| V. | ABKÜRZUNGSVERZEICHNIS | X |
| VI. | DIAGRAMMVERZEICHNIS | XIII |
| VII. | AUSGANGSLAGE | 1 |
| VIII. | AUFTRAG..... | 1 |
| | 1. AUFTRAGSBESCHREIBUNG | 1 |
| | 2. BEAUFTRAGTE | 2 |
| | 3. AUFTRAGGEBER | 2 |
| | 4. HYPOTHESEN | 2 |
| IX. | METHODISCHES VORGEHEN | 3 |
| X. | RECHTLICHE GRUNDLAGE | 3 |
| | 1. GESETZGEBUNGSPROZESS | 3 |
| | 2. ZWECK..... | 4 |
| | 3. INHALT DER WHISTLEBLOWING-RICHTLINIE..... | 4 |
| | 4. UMSETZUNG | 6 |
| XI. | EMPIRISCHE STUDIE | 7 |
| | 1. METHODIK..... | 7 |
| | 2. ADRESSATEN UND RÜCKLAUFQUOTE..... | 8 |
| | 3. STATISTISCHE AUSWERTUNG | 9 |
| | a. <i>Motive</i> | 12 |
| | b. <i>Meldekanäle</i> | 15 |
| | c. <i>Interne vs. Externe Dienstleister</i> | 18 |
| | d. <i>Unternehmensgrösse</i> | 21 |
| | e. <i>Schweizer Unternehmen</i> | 25 |
| XII. | FAZIT..... | 30 |
| XIII. | ANNEX | 32 |
| | 1. FRAGEBOGEN MIT AUSGEWÄHLTEN SUMMARISCHEN ERGEBNISSEN | 32 |
| | 2. DEDUKTIVE STATISTIKEN..... | 37 |
| | 3. ANMERKUNGEN UND KOMMENTARE | 41 |

III. Literaturverzeichnis

AGRESTI ALAN, An Introduction to Categorical Data Analysis, 2. Ed., New Jersey 2007

COLNERIC NINO/GERDEMANN SIMON, Die Umsetzung der Whistleblower-Richtlinie in deutsches Recht, Rechtsfragen und rechtspolitische Überlegungen, in: HSI-Schriftreihe, Bd. 34, Frankfurt am Main 2020

DZIDA BORIS/GRANETZNY THOMAS, Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen, NZA 2020, S. 1201 ff.

FORST GERRIT, Die Richtlinie der Europäischen Union zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowing-Richtlinie), EuZA 2020, S. 283 ff.

HAHN ANNE-CATHERINE, Die neue EU Whistleblower-Richtlinie – Handlungsbedarf für Schweizer Unternehmen?, RR-COMP 1 2020, S. 2 ff.

OESCH MATTHIAS, Europarecht, Band I, Grundlagen, Institutionen, Verhältnis Schweiz-EU, Bern 2015

PEARSON KARL, X. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling, in: Philosophical Magazine Series 5, 50:302 (1990) 157 ff.

SCHMOLKE KLAUS ULRICH, Die neue Whistleblower-Richtlinie ist da! Und nun?, NZG 2020, S. 5 ff.

UPTON GRAHAM/COOK IAN, Dictionary of Statistics, 2. Ed., Oxford 2008

IV. Materialienverzeichnis

BLUMER HELENE/BRETTI-RAINALTER JEANINE/HAUSER CHRISTIAN, Whistleblowing Report 2021, Chur 2021 (zit. Whistleblowing-Report)

Council of Europe, Protection of Whistleblowers, Recommendation CM/Rec (2014)7 and explanatory memorandum, <https://rm.coe.int/16807096c7>, zuletzt besucht am 16. Dezember 2021 (zit. Protection of Whistleblowers)

Datenschutzexperte.de, Die neue Whistleblowing Richtlinie, Wie geht es weiter mit dem Hinweisgeberschutzgesetz?, <https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/die-neue-whistleblowing-richtlinie/>, zuletzt besucht am 16. Dezember 2021.

MAK LUCA, Österreichs Regierung steht beim EU-Schutz von Hinweisgebern auf der Bremse, https://www.ots.at/presseaussendung/OTS_20210324_OTS0086/oesterreichs-regierung-steht-beim-eu-schutz-von-hinweisgebern-auf-der-bremse, zuletzt besucht am 16. Dezember 2021 (zit. EU-Schutz von Hinweisgebern)

ROSENTHAL DAVID, EU-Whistleblower-Richtlinie: Fallstricke für Schweizer Unternehmen, <https://www.vischer.com/know-how/blog/eu-whistleblower-richtlinie-fallstricke-fuer-schweizer-unternehmen-39050/>, zuletzt besucht am 16. Dezember 2021 (zit. Fallstricke)

SDA-Meldung vom 5. März 2020, Parlament lässt Whistleblower im Ungewissen, https://www.parlament.ch/de/services/news/Seiten/2020/20200305084532103194158159041_bsd044.aspx, zuletzt besucht am 16. Dezember 2021 (zit. SDA-Meldung vom 5. März 2020)

V. Abkürzungsverzeichnis

| | |
|-------|--|
| Abs. | Absatz |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung) |
| AG | Aktiengesellschaft |
| Art. | Artikel |
| AT | Österreich |
| Aufl. | Auflage |
| BLaw | Bachelor of Law |
| BMJV | Bundesministerium der Justiz und für Verbraucherschutz |
| bspw. | beispielsweise |
| bzgl. | bezüglich |
| bzw. | beziehungsweise |
| ca. | circa |
| CDU | Christlich-Demokratische Union |
| CH | Schweiz |
| CSU | Christlich-Soziale Union |
| D | Deutsch |
| d.h. | das heisst |
| DACH | Deutschland, Österreich und die Schweiz |
| Dr. | Doktor |
| DSGVO | 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) (Text von Bedeutung für den EWR) |
| Ed. | Edition |
| EU | Europäische Union |
| Whistleblowing-Richtlinie | Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden |
| f. / ff. | die Folgende(n) |
| FR | Französisch |
| gem. | gemäss |
| GmbH | Gesellschaft mit beschränkter Haftung |
| h | Stunde(n) |
| i.d.R. | in der Regel |
| IT | Italienisch |
| KMU | Kleine und mittlere Unternehmen |
| lit. | Litera |
| N | Anzahl |
| NSA | National Security Agency |
| Prof. | Professor |
| RR-Comp | Recht relevant. für Compliance Officers |
| Rz. | Randziffer |
| S. | Seite(n) |

| | |
|------|---|
| sog. | sogenannt |
| US | Vereinigte Staaten von Amerika |
| vgl. | vergleiche |
| vs. | versus |
| z.B. | zum Beispiel |
| ZHAW | Zürcher Hochschule für angewandte Wissenschaften |
| ZWC | Zentrum für Wettbewerbs- und Handelsrecht |

VI. Diagrammverzeichnis

| | |
|---|----|
| DIAGRAMM 1: ANZAHL MITARBEITENDE PER 31.10.2021..... | 22 |
| DIAGRAMM 2: (GEPLANTES) JAHR DER EINFÜHRUNG EINES HINWEISGEBERSCHUTZSYSTEMS | 27 |
| DIAGRAMM 3: VERTEILUNG BETRIEBSSTÄTTEN | 33 |
| DIAGRAMM 4: MOTIVE FÜR DIE IMPLEMENTIERUNG EINES HINWEISGEBERSCHUTZSYSTEMS | 35 |
| DIAGRAMM 5: RELEVANZ BETR. KOSTEN, EINFACHHEIT UND ANONYMITÄT..... | 36 |

VII. Ausgangslage

Spätestens mit den Enthüllungen Edward Snowdens aus dem Juni 2013 über die Massenüberwachung der NSA gegenüber den eigenen US-Bürgern wurde die weltweite Ordre public nachhaltig erschüttert. Der Begriff «Whistleblowing» hat anschliessend im öffentlichen Diskurs eine erhebliche Eigendynamik entwickelt.

Der daraus resultierende Trend zum besseren Schutz von Hinweisgebern hat sich in der EU neben der Initiative des Europarats zu einem Whistleblowing-Abkommen¹ auch in der Richtlinie 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (kurz «Whistleblowing-Richtlinie») manifestiert.² Die zwingende nationale Umsetzung der Direktive bis zum Stichtag am 17. Dezember 2021, stellt nicht nur die Mitgliedsstaaten vor massive Herausforderungen. So setzen sich auch zahlreiche Compliance-Abteilungen von Unternehmen mit der zum Teil stark auslegungsbedürftigen Whistleblowing-Richtlinie und deren rechtlichen Anforderungen auseinander.³

VIII. Auftrag

Das vorliegende Gutachten beschäftigt sich mit der Whistleblowing-Richtlinie, deren zu erwartender Umsetzung in nationales Recht und die diesbezügliche Unternehmenspraxis. Die **Parameter** stellen sich im Detail wie folgt dar:

1. Auftragsbeschreibung

Die ZHAW ist beauftragt die Auswirkungen der Whistleblowing-Richtlinie aus unternehmenstechnischer Perspektive für den Bereich Compliance zu analysieren. Insbesondere wird dabei untersucht, wie die Whistleblowing-Richtlinie von Unternehmen rezipiert wird. Neben dem Status quo in Bezug auf Hinweisgebersysteme, werden auch betriebliche Herausforderungen, sowie Ansprüche und Zukunftstendenzen hierzu erforscht.

¹ Council of Europe, Protection of Whistleblowers.

² DZIDA/GRANETZNY, S 1201.

³ FORST, S. 284.

2. Beauftragte

Die Beauftragte ist das Zentrum für Wettbewerbsrecht und Compliance (ZWC) der Zürcher Hochschule für angewandte Wissenschaften (ZHAW), Gertrudstrasse 15, 8400 Winterthur, Schweiz, welches in Lehre, Schulung und Weiterbildung auf den Rechtsgebieten des Wettbewerbsrechts und Compliance über schweizweit herausragendes Know-how verfügt.

3. Auftraggeber

Bei den Auftraggebern handelt es sich um die rechtlich eigenständigen Unternehmen TELAG AG, Hardturmstrasse 101, 8005 Zürich, Schweiz und Snubes GmbH, Prinzessinnenstrasse 19/20, 10969 Berlin, Deutschland. Die Unternehmen agieren miteinander in Form eines Joint Venture und haben in gemeinsamer Kooperation das Produkt «whistleTAG», eine ganzheitliche Komplettlösung für Unternehmen in Bezug auf Hinweisgebersysteme entwickelt.

4. Hypothesen

Zunächst wurden in Bezug auf die Forschungsfragen unterschiedliche Hypothesen aufgestellt. Diese Präsumtionen wurden unter die nachstehenden und auf Hinweisgebersysteme selbsterklärende Kategorien subsumiert und mittels empirischer Auswertung überprüft.

- **Motive**
 - **Hypothese 1:** Unternehmen installieren Hinweisgebersysteme aufgrund unternehmensinterner Gründe ebenso oft wie aufgrund einer gesetzlichen Vorschrift.
- **Meldekanäle**
 - **Hypothese 2:** Digitale Meldekanäle (E-Mail, Intranet, Internet) werden bevorzugt, weil sie sich besser in Prozessabläufe integrieren lassen.
 - **Hypothese 3:** Ombudsstellen werden nicht eingerichtet, weil sie die Anonymität der Hinweisgeber nicht gewährleisten können.
- **Interne vs. externe Dienstleister**
 - **Hypothese 4:** Externe Meldesysteme werden bevorzugt, weil sie Anonymität gewährleisten, weniger Kosten generieren und einfacher in den Prozessablauf integriert werden können und zudem ein höheres Serviceniveau sicherstellen.
- **Unternehmensgrösse**
 - **Hypothese 5:** Grosse Unternehmen sind weniger kostensensibel (als KMUs) und bevorzugen externe Meldesysteme.

- **Hypothese 6:** Grosse Unternehmen haben mit grösserer Wahrscheinlichkeit als KMUs Hinweisgebersysteme bereits implementiert.
- **Schweizer Unternehmen**
 - **Hypothese 7:** Schweizer Unternehmen (ohne Aktivitäten in der EU) bevorzugen externe Meldesysteme und haben andere Ansprüche an Serviceniveau und Ausgestaltung (Meldekanäle) als solche mit Aktivitäten in der EU.
 - **Hypothese 8:** Schweizer Unternehmen (ohne Aktivitäten in der EU) richten Hinweisgebersysteme später ein als andere Unternehmen (mit Aktivitäten in der EU), da für sie keine gesetzliche Pflicht dazu besteht.

IX. Methodisches Vorgehen

Die Erstellung des Gutachtens erfolgt in zwei wesentlichen Schritten:

- **Rechtliche Grundlage:** Zunächst wird die Whistleblowing-Richtlinie als massgebende rechtliche Grundlage analysiert. Es werden neben dem Zweck, auch die wichtigsten inhaltlichen Ausgestaltungen und die bisherigen Umsetzungsbestrebungen der Europäischen Mitgliedsstaaten beleuchtet. In Bezug auf den Geltungsbereich der Whistleblowing-Richtlinie wird neben den erheblichen Auswirkungen auf die Unionsländer auch auf solche gegenüber Drittstaaten ausserhalb der EU, wie bspw. die Schweiz, näher eingegangen.
- **Empirische Studie:** In der darauffolgenden empirischen Analyse wird zunächst die angewandte Untersuchungsmethode dargelegt. Vorgängig aufgestellte Hypothesen werden unter Auswertung der Forschungsergebnisse statistisch auf deren Gültigkeit überprüft. Die diesbezügliche Methodik wird unter XI. 1. genauer dargelegt.

X. Rechtliche Grundlage

1. Gesetzgebungsprozess

Das Europäische Parlament verabschiedete am 16. April 2019 die Whistleblowing-Richtlinie. Über die Verabschiedung der Richtlinie gab es lange Zeit interne Uneinigkeit zwischen den EU-Organen: Der Europäische Rat hat sich verstärkt gegen die auffallend hinweisgeberfreundliche Position des Europäischen Parlaments gestemmt. Nach medial durchgeführten Auseinandersetzungen zwischen den Institutionen ist schliesslich am 23.

Oktober 2019 der finale Text vom Präsidenten des Rats und dem Präsidenten des Parlaments förmlich verabschiedet worden.⁴ Seit der Veröffentlichung am 26. November 2019 haben die einzelnen Mitgliedsstaaten Zeit, die Bestimmungen in nationales Recht zu kodifizieren.⁵

2. Zweck

Das Ziel der Whistleblowing-Richtlinie wird bereits in dessen Artikel 1 Abs. 1 klar definiert: Der Rechtsakt dient primär dazu, für Hinweisgeber einen gewissen Mindestschutz zu gewährleisten. Whistleblower sollen ermutigt werden, Missstände und Rechtsverstöße in Unternehmen wie auch in Einrichtungen des öffentlichen Sektors – wie z.B. Gemeinden oder Behörden – zu melden. Es soll verhindert werden, dass potenzielle Whistleblower einem solchen Handeln aus Angst vor zukünftigen Repressalien, wie einer betriebsinternen oder aber auch öffentlichen Stigmatisierung nicht nachkommen.

Um diesem Schutz entsprechend gewährleisten zu können, verpflichtet die Richtlinie Unternehmen, welche unter dessen Geltungsbereich fallen, geeignete Meldekanäle bei gleichzeitigem, rechtlichem Schutz des Whistleblowers zur Verfügung zu stellen. Entgegen dem ursprünglichen Richtlinienentwurf welcher prioritär interne Meldekanäle vorsah, werden in der finalen Fassung interne und externe Meldekanäle gleichrangig behandelt.⁶

3. Inhalt der Whistleblowing-Richtlinie

a. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich umfasst gemäss Art. 2 der Whistleblowing-Richtlinie Meldungen zu Verstößen von Unionsrecht. Namentlich sind die wichtigsten erfassten Bereiche, solche des Steuerbetrugs, der Geldwäscherei, der Delikte im Zusammenhang mit öffentlichen Aufträgen, der Produkt- und Verkehrssicherheit, des Umweltschutzes, der öffentlichen Gesundheit sowie des Verbraucher- und Datenschutzes. Nicht erfasst werden Fehlverhalten wie etwa Diskriminierungen. Art. 8 Abs. 1 der Whistleblowing-Richtlinie schreibt vor, dass sowohl juristische Personen des privaten als auch des öffentlichen Sektors geeignete Meldesysteme für Hinweisgeber einrichten müssen. Durch die flächendeckende, horizontale Ausdehnung des Rechtsakts soll ein möglichst breit gefächerter Anwendungsbereich gewährleistet werden.⁷

⁴ SCHMOLKE, S. 5.

⁵ DZIDA/GRANETZNY, S. 1201.

⁶ DZIDA/GRANETZNY, S. 1203.

⁷ SCHMOLKE, S. 6.

b. Persönliche Anwendungsbereich

Der persönliche Anwendungsbereich ist gem. Artikel 4 Abs. 1 Whistleblowing-Richtlinie ebenfalls sehr breit gehalten. Der Kreis geschützter Personen umfasst neben Arbeitnehmenden gemäss Art. 45 AEUV und Selbstständigen nach Art. 49 AEUV, praktisch jede Art beruflicher Tätigkeit – selbst unbezahlte Praktikumsstellen.

c. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich ist in der Richtlinie nicht explizit geregelt. Aus Art. 4 Whistleblowing-Richtlinie lässt sich ableiten, dass die gesamte Tätigkeit bzw. der berufliche Kontext für den Anwendungsbereich relevant sind. Mit anderen Worten sind alle juristische Personen des privaten und öffentlichen Sektors zur Implementierung eines Meldesystems verpflichtet, wenn sie einer Tätigkeit im EU-Raum nachgehen und unter die weiteren Anwendungsvoraussetzungen (Grösse des Unternehmens, sachlicher Anwendungsbereich, etc.) fallen. Folglich werden Drittstaaten wie die Schweiz nur dann von den gesetzlichen Bestimmungen tangiert, wenn diese auch Betriebsstätten, Standorte oder andere Beziehungen in die EU unterhalten.⁸

d. Meldesysteme

Ab dem Stichtag zur nationalen Umsetzung ist es Aufgabe der Mitgliedsstaaten der EU dafür Sorge zu tragen, dass juristische Personen des Privatrechts ab 250 Mitarbeitenden, sowie auch juristische Personen des öffentlichen Sektors verpflichtet werden Meldesysteme einzuführen. Unternehmen, welche zwischen 50 und 249 Mitarbeitende beschäftigen, wurde eine Übergangsfrist von 2 Jahren gewährt.⁹

Bei der Schaffung der Hinweisgebersysteme steht es den jeweiligen Unternehmen frei, ob diese die verpflichtenden Meldekanäle unternehmensintern implementieren wollen oder auf ein Drittunternehmen setzen, welches diese extern betreibt und überwacht. Eine Meldung muss mindestens mündlich, schriftlich oder mittels physischem Zusammentreffen erfolgen können. Den Unternehmen wird dabei gesetzlich ein breites Instrumentarium unterschiedlicher Meldekanäle an die Hand gegeben. Erwähnt seien in diesem Zusammenhang eine Mitteilung an die zuständige Dienststelle, mittels Online-System, Postweg, Whistleblower-Hotline oder Anrufbeantwortersystem.

Erstaunlicherweise hat die EU jedoch nicht zwingend festgehalten, dass die Anonymität des Informanten von den Unternehmen garantiert werden muss. Zwar wird zum einen gesetzlich normiert, dass die Vertraulichkeit der Identität des Hinweisgebers gewahrt bleiben muss, so etwa gem. Art. 9 Abs. 1 lit. a, 12 Abs. 3

⁸ ROSENTHAL, Fallstricke.

⁹ BLUMER/BRETTI/HAUSER, Whistleblowing-Report.

und Art. 16 Whistleblowing-Richtlinie, und zum anderen die jeweils hinweisgebende Person auch vor Repressalien geschützt werden muss, Art. 1 Abs. 1 und Art. 19 Whistleblowing-Richtlinie. Dies unterscheidet sich jedoch – entgegen weit verbreiteter Ansicht – von der Anonymität eines Hinweisgebers: Sofern die Identität des Informanten bekannt ist, muss diese zur Erfüllung gesetzlicher Verpflichtungen wie z.B. strafrechtlichen Untersuchungsverfahren vom jeweiligen Unternehmen an die zuständigen Behörden offengelegt werden. Bei vollkommener und rückverfolgungsfreier Anonymität sind die Personendaten niemandem bekannt – selbst der zuständigen Meldestelle nicht.¹⁰

Interessanterweise sieht die EU zudem keine Kaskade an Meldestellen bzw. -stufen für den Whistleblower vor: Ein Whistleblower kann sich aussuchen, ob er die unternehmenseigene Whistleblowerlösung nutzt oder ob er sich direkt an die Behörden wendet. Hingegen muss nach Art. 15 der Whistleblowing-Richtlinie eine unmittelbare oder offenkundige Gefahr für das öffentliche Interesse bestehe, oder aber es zu befürchten sei, dass eine interne Meldung wirkungslos wäre bzw. Repressalien gegen den Hinweisgeber ergriffen würden, damit dieser sich ohne Umwege an die Öffentlichkeit wenden kann.¹¹

e. Sanktionen

Die Sanktionen der Richtlinie werden in Art. 23 Whistleblowing-Richtlinie geregelt. So werden Unternehmen bestraft, welche die Vertraulichkeit bezüglich der Identität des Whistleblowers verletzen, Meldungen behindern oder aber in Versuch kommen, sie zu behindern, Repressalien gegen Hinweisgeber ergreifen oder aber mutwillige Gerichtsverfahren gegen diese anstreben. Die Ausgestaltung des Sanktionsmechanismus unterliegt weitestgehend den Mitgliedsstaaten. Jedenfalls muss dieser aber eine ausreichend abschreckende Wirkung aufweisen um Verstöße generalpräventiv zu vermeiden.

4. Umsetzung

Bei der Umsetzung steht es den einzelnen nationalen Gesetzgebern frei, ob sie den Anwendungsbereich oder die Sanktionen der Direktive erweitern bzw. diese weiter verschärfen möchten.

¹⁰ COLNERIC/GERDEMANN, S. 139.

¹¹ HAHN, S. 2.

Mitte Februar 2021 hatten lediglich 1/3 der Mitgliedsstaaten mit der Umsetzung begonnen. Soweit ersichtlich, ist es derzeit ausgeschlossen, dass die 27 Mitgliedsstaaten (oder aber auch zumindest ein Grossteil davon) die Whistleblowing-Richtlinie rechtzeitig umsetzen können.

In vorreitender Funktion hat die Tschechische Republik bereits am 09. Februar 2021 dem Parlament einen Gesetzesentwurf vorgelegt.¹² Die Lage in der DACH-Region stellt sich gegenwärtig hierzu noch anders dar: In Deutschland wurde der Gesetzesentwurf aktuell noch nicht verabschiedet, obwohl schon Ende 2020 der Minister des Bundesministeriums für Justiz und Verbraucherschutz (BMJV) einen Gesetzentwurf vorgelegt hatte. Dieser wurde jedoch von der CSU / CDU gekippt. Unter anderem aufgrund der Bundestagswahlen und der sich daran anschliessenden zähen Koalitionsverhandlungen kann der Umsetzungstermin in der Bundesrepublik nicht eingehalten werden. Es wird wohl darauf hinauslaufen, dass in dieser Zeit, ohne nationale Gesetzgebung, auf die EU-Direktive zurückgegriffen wird, damit überhaupt ein Urteil gefällt werden kann.¹³

Ein Blick nach Österreich zeigt, dass Details zum Umsetzungsprozess, trotz mehrfacher Anfragen verschiedener relevanter Stellen, nicht bekannt gegeben werden.¹⁴

Die einzelnen Mitgliedsstaaten laufen somit Gefahr, sich in einem Vertragsverletzungsverfahren der EU auszusetzen.¹⁵

Auch in der Schweiz wurde im März 2020 über eine Normierung des Whistleblowerschutzes abgestimmt. Der Nationalrat lehnte die Vorlage allerdings ab. Unter anderem sei der (nachgebesserte) Entwurf zu technokratisch gewesen und würde nur noch mehr Rechtsunsicherheit schaffen.¹⁶

XI. Empirische Studie

1. Methodik

Zur Beantwortung des Forschungsauftrags wurde eine Umfrage mittels Fragebogen unter den Kunden der TELAG AG und Snubes GmbH durchgeführt. Die Kunden wurden per E-Mail kontaktiert und um eine Teilnahme an der Umfrage gebeten.

¹² MAK, EU-Schutz von Hinweisgebern.

¹³ Datenschutzexperte.de, S. ?

¹⁴ MAK, EU-Schutz von Hinweisgebern.

¹⁵ OESCH, Rz. 556 ff.

¹⁶ SDA-Meldung vom 5. März 2020.

Die jeweiligen E-Mails wurden personalisiert versendet und jeweils mit einem individuellen Link für den Zugriff auf den Onlinefragebogen versehen. Dadurch konnte sichergestellt werden, dass es keine Mehrfachteilnahmen gab.

Die Umfrage konnte in der Zeit vom 16.11. bis zum 30.11.2021 beantwortet werden. Um die Teilnahme zu erhöhen, wurde erstmalig am 20.11.2021 und anschliessend erneut am 26.11.2021 per E-Mail an die Möglichkeit zur Teilnahme erinnert.

Aus Anonymitätsgründen können die Antworten den jeweiligen Umfrageteilnehmern nicht zugeordnet werden. Im offenen Teil des Fragebogens bestand jedoch die Möglichkeit, eine E-Mail-Adresse für die Zusendung der Studienergebnisse anzugeben. In diesen Fällen haben die Teilnehmer bewusst auf eine entsprechende Anonymität verzichtet.

Der Fragebogen umfasst insgesamt sechs Teile.

- Im **ersten Teil** wurden kennzeichnende soziodemografische Merkmale (Anzahl Mitarbeitende, geografische Aktivitäten) der Unternehmen erhoben.
- Im **zweiten Teil** wurden weitere (voraussichtlich nationale) Voraussetzungen für eine rechtliche Pflicht zur Einrichtung eines Meldesystems abgefragt (Umsatzgrenze), sowie ob ein Meldesystem bereits vorhanden ist.
- Im **dritten Teil** sollten Angaben zum Zeitraum einer allfällig geplanten Etablierung eines Meldesystems gemacht werden.
- Im **vierten Teil** wurden die Teilnehmer nach den Motiven für die Implementierung eines «Whistleblowing»-Systems befragt.
- Im **fünften Teil** wurden die Adressaten um Angaben zu den wünschenswerten Eigenschaften, zu Meldekanälen und dem gewünschten Serviceniveau eines Meldesystems gebeten und zur Frage, ob sie ein internes oder externes Meldesystem bevorzugen.
- Im **sechsten und finalen Teil** schliesslich konnten freie Anmerkungen beigefügt werden, sowie, wie vorgängig bereits erwähnt, eine E-Mail-Adresse für den Bezug der Studienergebnisse hinterlassen werden.

Der gesamte Fragebogen mit den summarischen Resultaten ist im Anhang dokumentiert.

2. Adressaten und Rücklaufquote

Für die Umfrage wurden vom Auftraggeber 7487 E-Mail-Adressen zur Verfügung gestellt. Aus unterschiedlichen Gründen konnten nicht alle Adressaten erreicht werden, so dass die effektive Stichprobe 5702 Teilnehmer umfasste. Von diesen beteiligten sich 366 an der Umfrage, was einer Beteiligungsquote von 6.4 Prozent entspricht.

Mehr als die Hälfte der Antwortenden hat die Umfrage abgebrochen, 149 haben sie beendet. Von diesen waren drei so genannte «Tester», d.h. Teilnehmer zu Testzwecken und zur Qualitätskontrolle. Damit standen insgesamt 146 komplett ausgefüllte Fragebögen für die Auswertung zur Verfügung. Zu Abbrüchen kam es fast ausschliesslich bei den ersten beiden Fragen, so dass die unvollständigen Antwortbögen kaum Einfluss auf die Beobachtungszahl bei den einzelnen Fragen haben. Die folgende Tabelle bietet eine zusammenfassende Übersicht der Stichprobe.

Umfrage Hinweisgebersystem

| | | | |
|---|-------------------------|-------|--------------|
| Anzahl Teilnehmer (Stichprobe «Brutto 1») | | | 7487 |
| <i>Ausfälle</i> | | | 1785 |
| | nicht erreichbar | 504 | |
| | E-Mail nicht zustellbar | 1281 | |
| Effektive Stichprobe («Brutto 2») | | | 5702 |
| <i>Beteiligung</i> | | | 366 |
| | beendet | 149 | |
| | unterbrochen | 217 | |
| Beteiligungsquote (bezogen auf «Brutto 2») | | | 6.42% |
| | beendet | 2.61% | |
| | unterbrochen | 3.81% | |

Es wird davon ausgegangen, dass die 146 vollständigen Fragebögen zufällige und unabhängige Beobachtungen repräsentieren und somit einer statistischen, deduktiven Analyse zugänglich sind. Der Stichprobenumfang rechtfertigt grundsätzlich die Verwendung von Statistiken der grossen Zahl (sog. «asymptotische Statistiken»).

3. Statistische Auswertung

Die Auswertung der eingegangenen Antworten erfolgt mittels beschreibender sowie schliessender Statistik. Dazu werden die Antworthäufigkeiten berechnet sowie die verschiedenen Antworten zueinander in Beziehung gesetzt. Dadurch ist es zum Beispiel möglich, Aussagen darüber zu treffen, ob es Zusammenhänge zwischen der geografischen Präsenz von Unternehmen und deren Ansprüche an Meldesysteme gibt.

Die Zusammenhänge werden mittels eines statistischen Tests darauf geprüft, ob sie nur zufällig sind, oder ob der Zufall mit ausreichend hoher Wahrscheinlichkeit verworfen werden kann. Verworfen werden soll, wenn die Irrtumswahrscheinlichkeit (sog. «Signifikanzniveau») fünf Prozent oder weniger beträgt. Ist das der Fall, so ist der untersuchte Zusammenhang mit hoher Gewissheit tatsächlich vorhanden und beruht nicht auf einem blossen Zufall. Die Irrtumswahrscheinlichkeit von fünf Prozent sagt aus, dass es sein kann, dass bei fünf von hundert Tests der geprüfte Zusammenhang trotz eines signifikanten Testergebnisses in Wirklichkeit nicht besteht.

Am folgenden Beispiel sei das Vorgehen illustriert. Grundlage bildet die Nullhypothese:

Hypothese (0): Es gibt keinen Zusammenhang zwischen geografischer Präsenz eines Unternehmens und dem «Grund X» für die Einführung eines Meldesystems.

Diese Hypothese wird dann für jeden einzelnen «Grund X» gegen die Alternativhypothese getestet:

Hypothese (1): Es gibt keinen Zusammenhang zwischen geografischer Präsenz eines Unternehmens und dem «Grund X» für die Einführung eines Meldesystems. Als «Grund X» werden einzeln die im Fragebogen vorgegebenen Antworten getestet.

Der Test ist der so genannte «Chi-Quadrat-Unabhängigkeitstest», der auch auf kategoriale Variablen, wie z.B. der geografischen Präsenz, angewendet werden kann.¹⁷ Die Nullhypothese wird verworfen, wenn der Testwert des «Chi-Quadrat-Unabhängigkeitstest» eine bestimmte Schwelle überschreitet. Diese Schwelle wird so gewählt, dass nur in fünf von einhundert Fällen eine falsche Testentscheidung gefällt wird. Dieser Fehler besteht darin, dass kein Zusammenhang vorliegt, obwohl die Teststatistik einen solchen Zusammenhang anzeigt. Dieser Fehler wird auch Fehler erster Art genannt.

Die Ergebnisse werden in Kreuztabellen nach folgender Mustertabelle zusammengefasst:

| | <i>In welchen Ländern hat Ihr Unternehmen Betriebsstätten?</i> | | | | | |
|--|---|--------------|-----------|------------------|-----------------|---------------|
| <i>Warum implementieren Sie ein Hinweisgeberschutzsystem?</i> | CH | D | AT | EU andere | Nicht EU | nur CH |
| <i>wegen einer gesetzlichen Pflicht</i> | 43.6% | 64.6% | 60.6% | 62.8% | 59.1% | 35.3% |
| <i>um Sanktionen zu verhindern</i> | 18.1% | 38.5% | 30.3% | 39.5% | 36.4% | 9.8% |

¹⁷ PEARSON, 157 ff.; vgl. Auch AGRESTI, Abschnitt 2.4.

| | | | | | | |
|--|--------------|--------------|-------|--------------|--------------|-------|
| <i>um Reputationsschäden zu vermeiden</i> | 51.1% | 53.8% | 51.5% | 72.1% | 61.4% | 43.1% |
| <i>um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein</i> | 69.1% | 60.0% | 63.6% | 81.4% | 70.5% | 66.7% |
| <i>um die Wettbewerbsfähigkeit des Unternehmens zu steigern</i> | 17.0% | 27.7% | 27.3% | 37.2% | 40.9% | 9.8% |
| <i>andere Gründe</i> | 9.6% | 4.6% | 9.1% | 4.7% | 2.3% | 13.7% |

Die vorstehende Tabelle ist wie folgt zu lesen:

- (i) In den vertikalen Spalten sind die Antworten derjenigen Teilnehmer eingetragen, die auf die Frage «In welchen Ländern hat Ihr Unternehmen Betriebsstätten?» als Antwort jeweils die Spaltenüberschrift angekreuzt hatten, also etwa «CH» für «in der Schweiz» oder «EU andere» für «weitere EU-Länder». Die Kategorie «nur CH» wurde aus denjenigen Antworten gebildet, bei welchen neben «Schweiz» keine weitere Kategorie angegeben wurde.
- (ii) In den horizontalen Reihen sind die Kategorien der Gründe für die Implementierung eines Hinweisgebersystems erfasst, wie bspw., «um Reputationsschäden zu vermeiden».

Die Schnittstellen aus «Land» und «Grund» können demnach folgendermassen aufgefasst werden: 43.6 Prozent derjenigen Teilnehmer, die als Land, in dem sich eine Betriebsstätte des Unternehmens befindet, «Schweiz» angekreuzt haben, führen ein Hinweisgebersystem aufgrund einer gesetzlichen Pflicht ein. Da diese Kategorie auch Unternehmen erfasst, die ebenfalls in Deutschland oder einem anderen EU-Land tätig sind, ist dieser Wert höher als die 35.3% für die Betriebe, die ausschliesslich in der Schweiz tätig sind (Spalte «nur CH», selbe Zeile).

Die zugehörigen statistischen Hypothesen unterstellen nun jeweils, dass kein Zusammenhang zwischen den Kategorien «Land» und «Grund» bestehe. Die Nullhypothese «Es gibt keinen Zusammenhang zwischen der Tatsache, dass ein Unternehmen nur in der Schweiz tätig ist (Kategorie «Land») und der Nennung des Grundes «gesetzliche Pflicht» (Kategorie «Grund»)» bedeutet etwa, dass der Grund «gesetzliche Pflicht» unabhängig davon angegeben wird, egal, ob ein Unternehmen ausschliesslich in der Schweiz tätig ist, oder nicht.

Das Testergebnis ist in diesem Beispiel durch Dekoration des Schriftbildes des Tabelleneintrags wiedergegeben. Ist die jeweilige Prozentzahl fett gedruckt bedeutet das, dass die zugehörige Nullhypothese auf dem vorgegebenen Signifikanzniveau von fünf Prozent

abgelehnt wurde. Für den vorliegenden Fall bedeutet dies, dass sich die Unternehmen, die ausschliesslich in der Schweiz aktiv sind, bezüglich des Grundes «gesetzliche Pflicht» statistisch signifikant von denjenigen unterscheiden, die nicht in der Schweiz tätig sind. Damit besteht ein Zusammenhang zwischen der Tatsache, dass ein Unternehmen in der Schweiz tätig ist und der Angabe des Grundes «gesetzliche Pflicht».

Mit dieser Beobachtung allein kann allerdings nicht gesagt werden, welche Richtung dieser Zusammenhang hat, d.h., ob Schweizer Unternehmen eher häufiger diesen Grund angeben haben als nicht Schweizer Unternehmen oder umgekehrt. Diese Richtung kann jedoch wie folgt aus den Tabellenwerten abgeleitet werden: Wenn 35.3 Prozent dieser Unternehmen diesen Grund angegeben haben, haben es 64.7 Prozent nicht getan. Der Wert von 35.3 Prozent ist gemäss Teststatistik entsprechend statistisch signifikant kleiner als 64.7 Prozent.

Es muss dabei beachtet werden, dass die Teststatistik auf den Beobachtungen aller vier denkbaren Kombinationen aus «gesetzliche Pflicht als Grund genannt» / «gesetzliche Pflicht als Grund nicht genannt» sowie «nur in der Schweiz tätig» / «nicht ausschliesslich in der Schweiz tätig» beruht. Die Prozentzahlen in der Tabelle geben zur besseren Wahrung der Übersichtlichkeit lediglich die bedingten Anteile (bedingt auf das Land) an. Dadurch können auch sehr kleine (nahe Null) oder sehr grosse (nahe 100 Prozent) Prozentangaben «nicht signifikant» sein. Ein weiterer Einflussfaktor ist die Anzahl der Beobachtungen, die je nach Antwortkategorie schwanken kann.

In Abhängigkeit vom jeweiligen Zusammenhang werden die Irrtumswahrscheinlichkeiten der getesteten Hypothesen als «p-Wert» separat angegeben, sowie Angaben zur Anzahl der Beobachtungen gemacht. Im Beispielfall wurde darauf verzichtet, die zugehörigen Freiheitsgrade der Tests anzugeben, um die Übersichtlichkeit zu wahren.

Im Folgenden werden die Ergebnisse für die verschiedenen interessierenden Zusammenhänge präsentiert.

a. Motive

Es ist von entscheidender Bedeutung zunächst festzustellen was die treibenden Faktoren in Bezug auf die Installation eines Meldesystems sind. Insbesondere scheint hierzu die Abgrenzung zwischen einer zwingenden, gesetzlichen Verpflichtung und einer freiwilligen Implementierung besonders interessant. Mit der nachfolgend aufgestellten Hypothese wird die Motivation der Unternehmen diesbezüglich ergründet.

(1) Hypothese

Hypothese 1: Unternehmen installieren Hinweisgebersysteme aufgrund unternehmensinterner Gründe ebenso oft wie aufgrund einer gesetzlichen Vorschrift.

(2) Plausibilitätstest

Kriterien: Um herauszufinden, welche Kriterien für Unternehmen ausschlaggebend sind, ein Hinweisgebersystem zu implementieren, wurden folgende (freiwillige und verpflichtende) Aspekte in der Umfrage verwendet:

- Vermeidung von Reputationsschäden (freiwillig)
- Transparenz der Unternehmenskultur (freiwillig)
- Steigerung der Wettbewerbsfähigkeit (freiwillig)
- Gesetzliche Pflichten (verpflichtend)
- Sanktionsverhinderung (freiwillig / verpflichtend)
- Sonstige Gründe

Fragen: Zur Überprüfung der Hypothese wurde den Umfrageteilnehmern folgende Frage gestellt:

- Warum implementieren Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz)?

(3) Erkenntnisse

Gemäss den Rückmeldungen ist gerade die Unternehmenskultur ein wichtigerer Grund für die Einführung eines Hinweisgebersystems als die gesetzliche Pflicht. Mit 61.6 Prozent der Nennungen ist die Antwort «um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein» populärer als «wegen einer gesetzlichen Pflicht», die von insgesamt 52.1 Prozent der Umfrageteilnehmer genannt wird. Mit Hilfe eines statistischen Tests können die Unterschiede in den Antworten auf statistische Signifikanz geprüft werden. Dazu werden die Antworten paarweise mit Hilfe des nichtparametrischen sog. «Wilcoxon-Rang-Tests» verglichen.¹⁸ Im genannten Vergleich konnte die Hypothese, dass kein Unterschied besteht, nicht verworfen werden (p-Wert= 0.44). Die Antwort «wegen einer gesetzlichen Pflicht» kann auch mit den übrigen Antwortoptionen verglichen werden.

Die nachfolgende Tabelle zeigt die Ergebnisse dieser Analyse: Verglichen werden dabei die Häufigkeiten der verschiedenen Antworten auf die Frage «Warum implementieren Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz)?» mit der Häufigkeit der Nennung der Antwort «wegen einer gesetzlichen Pflicht». Dabei erweist sich der Unterschied in der Häufigkeit bzgl. der Antwortmöglichkeiten «um Sanktionen zu verhindern», «um die Wettbewerbsfähigkeit des Unternehmens zu steigern» sowie «andere Gründe» als statistisch signifikant. Bei den Optionen «um Reputationsschäden zu vermeiden» und «um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein» liegt hingegen nicht

¹⁸ Vgl. etwa Upton/Cook, Wilcoxon signed-rank tests.

genügend Evidenz vor, um die Nullhypothese, dass keine Unterschiede bestehen, zu verwerfen.

Warum implementieren Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz)?

| N=146 | Prozent | p-Wert |
|--|---------|--------------|
| <i>wegen einer gesetzlichen Pflicht</i> | 52.1% | – |
| <i>um Sanktionen zu verhindern</i> | 26.0% | 0.000 |
| <i>um Reputationsschäden zu vermeiden</i> | 47.3% | 0.442 |
| <i>um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein</i> | 61.6% | 0.144 |
| <i>um die Wettbewerbsfähigkeit des Unternehmens zu steigern</i> | 17.8% | 0.000 |
| <i>andere Gründe</i> | 8.2% | 0.000 |

Wie unter XI. 3. bei der Beschreibung der statistischen Methode bereits diskutiert, kann weiterhin aufgezeigt werden, dass sich die Motive für die Einführung von Meldesystemen teilweise nach dem Land der Unternehmenstätigkeit unterscheiden lassen. Dass in den Unternehmen der EU, in welchen die gesetzliche Pflicht der Richtlinie besteht, das Motiv «wegen einer gesetzlichen Pflicht» relativ häufiger genannt wird als in Unternehmen mit Sitz in der Schweiz oder einem anderen Nicht-EU-Land war zu erwarten, da für letztere Beiden keine gegenwärtige gesetzliche Obligation besteht. Die Nullhypothese, dass die gesetzliche Pflicht relativ zu den anderen Ländern statistisch die gleiche Bedeutung hat, kann für Deutschland und die Schweiz abgelehnt werden. Das bedeutet, dass davon ausgegangen werden kann, dass Unternehmen, die eine Betriebstätigkeit in der Schweiz oder in Deutschland haben, statistisch signifikant andere Motive für die Einführung von Meldesystemen haben als die übrigen Unternehmen. An dem Befund, dass die unternehmensinternen Gründe ähnlich wichtig sind wie eine gesetzliche Pflicht, ändert sich dadurch jedoch nichts.

(4) Würdigung

Diese Ergebnisse deuten darauf hin, dass in der Tat unternehmensinterne Motive für die Einführung eines Meldesystems genauso relevant sind wie die gesetzliche Pflicht.

Selbst wenn die Analyse der Motive sich ausschliesslich auf diejenigen Unternehmen beschränkt, die in der EU tätig sind, ändern sich die Testentscheidungen nicht. Dies bedeutet, dass auch für die Teilstichprobe der Unternehmen mit Tätigkeit in der EU gilt, dass das Motiv «gesetzliche Pflicht» statistisch gesehen genauso häufig genannt wird wie die Motive «um

Reputationsschäden zu vermeiden» und «um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein».

Daraus lässt sich zum einen ableiten, dass intern, mittels einer transparenten Unternehmenskultur, vorbildlich gegenüber Stakeholdern und Mitarbeitenden aufzutreten werden soll. Gleichzeitig soll zudem aber auch die Aussendarstellung am Markt und die Imagewirkung des jeweiligen Unternehmens in Öffentlichkeit und Medien gefördert werden.

Die Hypothese 1 kann insgesamt bestätigt werden.

b. Meldekanäle

(1) Hypothesen

Whistleblowersysteme müssen Kommunikationskanäle für die Meldung von Rechtsverstößen bereitstellen, die mit unterschiedlichen Kommunikationsgeschwindigkeiten, Absicherungen und Reaktionszeiten verbunden sind. Damit stellt sich die Frage, welche Kanäle Unternehmen bevorzugen. Für diese Entscheidung erschienen die folgenden beiden Hypothesen plausibel, die anhand der vorliegenden Stichprobe überprüft werden.

Hypothese 2: Digitale Meldekanäle (E-Mail, Intranet, Internet) werden bevorzugt, weil sie sich besser in Prozessabläufe integrieren lassen.

Hypothese 3: Ombudsstellen werden nicht eingerichtet, weil sie die Anonymität der Hinweisgeber nicht gewährleisten können.

(2) Plausibilitätstest

Kriterien: Die Unternehmen sollten bewerten, auf welche Arten von Meldekanälen und auf welche Eigenschaften ebendieser sie besonderen Wert legen.

- Digitale Meldekanäle wie E-Mail, Intranet oder Internet
- Telefonischer Meldekanal
- Einrichtung einer Ombudsstelle
- Kostenintensität der Meldekanäle
- Einfachheit der Prozesseinbettung
- Anonymität des Hinweisgebers

Fragen: Den Umfrageteilnehmern wurden in Bezug auf vorstehende Kriterien folgende Fragen gestellt:

- «Welche Meldekanäle sind Ihnen besonders wichtig?»
- «Welche Bedeutung haben für Sie die folgenden Eigenschaften (Kosten, Einfachheit, Anonymität) bei der Beschaffung eines Hinweisgeberschutzsystems?»

(3) Erkenntnisse

| Welche Meldekanäle sind Ihnen wichtig? | Prozent | N |
|---|---------|-----|
| E-Mail | 74.0% | 146 |
| Telefon | 38.4% | 146 |
| Intranet | 44.5% | 146 |
| Einrichtung einer Ombudsstelle für juristische Fragen | 32.2% | 146 |
| Internet | 41.8% | 146 |

Gemäss den Antworten der Teilnehmenden ist die E-Mail der mit Abstand (74 Prozent Nennungen) wichtigster Kanal, während eine Ombudsstelle (32 Prozent) als wenig relevant angesehen wird. Nachfolgende Tabelle analysiert die Bedeutung der Eigenschaften von Meldekanälen in Bezug auf die unterschiedlichen Meldekanäle selbst:

| <u>Bedeutung Eigenschaften x Meldekanäle</u> | | | | | | |
|--|---|----------------|-----------------|---------------------------|-----------------|-------|
| | Welche Meldekanäle sind Ihnen wichtig? | | | | | |
| | <i>E-Mail</i> | <i>Telefon</i> | <i>Intranet</i> | <i>Ombuds- stelle</i> | <i>Internet</i> | |
| Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems? | | | | | | |
| <u>Kosten</u> | | | | | | |
| <i>unwichtig</i> | 1 | 5.7% | 5.6% | 1.6% | 4.4% | 6.8% |
| | 2 | 8.5% | 9.3% | 11.1% | 13.3% | 8.5% |
| | 3 | 36.8% | 48.1% | 42.9% | 46.7% | 28.8% |
| | 4 | 24.5% | 20.4% | 28.6% | 24.4% | 25.4% |
| <i>sehr wichtig</i> | 5 | 24.5% | 16.7% | 15.9% | 11.1% | 30.5% |
| | N | 106 | 54 | 63 | 45 | 59 |
| | p-Wert | 0.16 | 0.115 | 0.023 | 0.05 | 0.798 |
| <u>Einfachheit der Prozesseinbettung</u> | | | | | | |

| | | | | | | |
|---|---------------|-------|-------|-------|-------|-------|
| <i>unwichtig</i> | 1 | 1.9% | 3.6% | 0.0% | 2.2% | 1.7% |
| | 2 | 1.0% | 1.8% | 1.6% | 0.0% | 0.0% |
| | 3 | 9.5% | 16.1% | 7.8% | 13.3% | 5.1% |
| | 4 | 29.5% | 30.4% | 34.4% | 28.9% | 20.3% |
| <i>sehr wichtig</i> | 5 | 58.1% | 48.2% | 56.3% | 55.6% | 72.9% |
| | N | 105 | 56 | 64 | 45 | 59 |
| | p-Wert | 0.156 | 0.054 | 0.107 | 0.769 | 0.043 |
| <u>Anonymität für den Hinweisgeber</u> | | | | | | |
| <i>unwichtig</i> | 1 | 3.7% | 1.8% | 1.5% | 0.0% | 3.3% |
| | 2 | 4.6% | 1.8% | 3.1% | 4.3% | 0.0% |
| | 3 | 8.3% | 10.7% | 3.1% | 4.3% | 9.8% |
| | 4 | 19.4% | 25.0% | 21.5% | 27.7% | 19.7% |
| <i>sehr wichtig</i> | 5 | 63.9% | 60.7% | 70.8% | 63.8% | 67.2% |
| | N | 108 | 56 | 65 | 47 | 61 |
| | p-Wert | 0.1 | 0.326 | 0.121 | 0.211 | 0.244 |

Zwischen den bevorzugten Meldekanälen und den zuvor erwähnten Eigenschaften besteht kaum ein Zusammenhang. Die Wahl eines bestimmten Meldekanals erfolgt folglich nicht aus Kostengründen oder weil er im besonderen Masse die Anonymität der Hinweisgeber schützen kann. Ebenso besteht nach Ansicht der Umfrageteilnehmer kein signifikanter Zusammenhang zwischen Meldekanal und Gewährleistung der Anonymität. Das bedeutet, dass alle Kanäle hinsichtlich der Gewährung der Anonymität der Hinweisgeber gleich stark bevorzugt bzw. abgelehnt werden.

Es lässt sich jedoch beobachten, dass diejenigen, für welche eine Ombudsstelle als Meldekanal wichtig ist, weniger sensibel für Kosten sind als die anderen Unternehmen. Ausserdem gaben jene, die das Internet als wichtigen Kanal betrachten, an, dass sie überdurchschnittlich viel Wert legen auf eine einfache Einbindung in die betriebsinternen Prozesse.

(4) Würdigung

Damit findet die 2. Hypothese im Wesentlichen keine Bestätigung, denn mit Ausnahme des «Meldekanals Internet» lässt sich kein statistisch signifikanter Zusammenhang zwischen Wahl des Kanals und Bedeutung der Einfachheit der Prozesseinbettung herstellen.

Hypothese 3 lässt sich ebenfalls nicht bestätigen. Die Anonymität der Hinweisgeber scheint mit keiner der Meldekanäle in Zusammenhang gebracht zu werden – auch nicht mit Ombudsstellen. Hingegen werden Ombudsstellen – wie auch der Meldekanal «Intranet» – statistisch signifikant in einen Zusammenhang mit den Kosten für Meldesysteme gestellt.

c. Interne vs. Externe Dienstleister

(1) Hypothese

Für jedes Unternehmen stellt sich bei der Einrichtung eines Meldesystems die Wahl zwischen «intern» und «extern»; eine Grundsatzentscheidung mit langfristigen Folgen. Die nachstehende Hypothese unterstellt, dass diese Entscheidung mit den gewünschten Eigenschaften zum Hinweisgebersystem in Verbindung steht.

Hypothese 4: Externe Meldesysteme werden bevorzugt, weil sie Anonymität gewährleisten, weniger Kosten generieren und einfacher in den Prozessablauf integriert werden können und zudem ein höheres Serviceniveau sicherstellen.

(2) Plausibilitätstest

Kriterien: Um aus Unternehmenssicht Vor- und Nachteile externer Meldesysteme gegenüber solcher internen Art miteinander abzuwägen, wurden Daten zu folgenden Kriterien erhoben:

- Kostenintensität der Meldekanäle
- Einfachheit von Meldesystemen
- Anonymität des Hinweisgebers
- Serviceniveau (wie bspw. DSGVO-Konformität, kurze Reaktionszeiten bei Meldungen etc.)

Fragen: Um die Hypothese auf ihre Validität hin zu überprüfen, wurden folgende Fragen gestellt:

- «Welche Bedeutung haben für Sie die folgenden Eigenschaften (Kosten, Einfachheit, Anonymität) bei der Beschaffung eines Hinweisgeberschutzsystems?»
- «Welches Serviceniveau ist Ihnen wichtig?»
- «Bevorzugen Sie ein Hinweisgeberschutzsystem betriebsintern aufzubauen oder einen externen Dienstleister?»

(3) Erkenntnisse

Zeigen sich bei den Antworten in Bezug auf Kosten und Einfachheit zwischen internen und externen Meldesystemen keine signifikanten Unterschiede, so unterscheiden sich diese in Bezug auf die Anonymität deutlich. Hierzu teilten ca. 92 Prozent der Befragten mit, welche die Anonymität einer Meldestelle mit «wichtig» oder «sehr wichtig» angegeben haben, dass sie

einen externen Anbieter bevorzugen. Im Vergleich dazu sprachen sich lediglich 78 Prozent für eine interne Meldestelle aus.

| <u>Bedeutung Eigenschaften x Intern versus extern</u> | | | | | | | |
|---|---------------|---|-------|-------|---------------------|-------|----|
| | | <i>Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems?</i> | | | | | |
| <i>Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister?</i> | | | | | | | |
| | | <u>Kosten</u> | | | | | |
| | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |
| | | 1 | 2 | 3 | 4 | 5 | N |
| p-Wert=0 | intern | 6.2% | 7.4% | 35.8% | 24.7% | 25.9% | 81 |
| | extern | 3.4% | 10.3% | 34.5% | 20.7% | 31.0% | 58 |
| | | | | | | | |
| | | <u>Einfachheit der Prozesseinbettung</u> | | | | | |
| | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |
| | | 1 | 2 | 3 | 4 | 5 | N |
| p-Wert=0.001 | intern | 2.5% | 2.5% | 11.4% | 25.3% | 58.2% | 79 |
| | extern | 5.1% | 0.0% | 6.8% | 32.2% | 55.9% | 59 |
| | | | | | | | |
| | | <u>Anonymität für den Hinweisgeber</u> | | | | | |
| | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |
| | | 1 | 2 | 3 | 4 | 5 | N |
| p-Wert=0 | intern | 6.1% | 6.1% | 9.8% | 20.7% | 57.3% | 82 |
| | extern | 3.3% | 0.0% | 4.9% | 21.3% | 70.5% | 61 |

Auch die erfragten Serviceaspekte «24h-Erreichbarkeit», «kurze Reaktionszeit», «Lösungen und Empfehlungen» und «DSGVO-Konformität» spielen keine Rolle für die Entscheidung zwischen internen und externen Systemen, wie die folgende Tabelle darlegt:

| | Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister? | | | |
|---|--|---------------|----------|---------------|
| | <u>intern</u> | <u>extern</u> | <i>N</i> | <i>p-Wert</i> |
| Welches Serviceniveau ist Ihnen wichtig? | | | | |
| <i>24h-Erreichbarkeit</i> | 56.0% | 44.0% | 143 | 0.88 |
| <i>kurze Reaktionszeit</i> | 57.8% | 42.2% | 143 | 0.85 |
| <i>Lösungen und Empfehlungen</i> | 53.1% | 46.9% | 143 | 0.36 |
| <i>DSGVO-Konformität</i> | 52.8% | 47.2% | 143 | 0.16 |
| <i>Mehrsprachigkeit</i> | 41.7% | 58.3% | 143 | 0.00 |

Den Antworten der Umfrageteilnehmer zufolge haben jene Unternehmen, die beispielsweise «24-Stunden-Erreichbarkeit» als wichtig erachten, eine leichte Präferenz für interne Meldesysteme. Das Gleiche gilt für die Aspekte «kurze Reaktionszeit», «Lösungen und Empfehlungen» und «DSGVO-Konformität». Statistisch signifikant korreliert lediglich die «Mehrsprachigkeit» im Zusammenhang mit der Wahl eines externen Anbieters.

(4) Würdigung

Dass Unternehmen hinsichtlich der Anonymität vorgängig externe Meldestellen präferieren, kann damit erklärt werden, dass sie befürchten, dass bei internen Systemen mittels «Datenlacks» oder mittels Zugriffs von unberechtigten Drittpersonen die Anonymität der Whistleblower gefährdet werden könnte.

Externe Bertreiber von Meldekanälen können in der Regel aufgrund ihrer meist über Jahre hinweg angesammelten Branchenerfahrung, eingespielten Fachprozessen und spezifischem Know-How eine erhöhte Vertraulichkeit gewährleisten. Zudem sind sie bei Nichteinhaltung i.d.R. direkt haftbar.

Die Tendenz zu externen Anbietern von Meldesystemen in Bezug auf die Mehrsprachigkeit kann so erklärt werden, dass Unternehmen davon überzeugt sind, die übrigen Serviceleistungen in genügender Qualität eigenständig produzieren zu können.

Die Hypothese 4 lässt sich somit nur teilweise bestätigen. Einerseits trifft es zu, dass die Wahrung der Anonymität (extern) eine statistisch signifikante Rolle bei der Entscheidung

zwischen externen und internen Systemen spielt. Hinsichtlich der Kosten und der Einfachheit der Implementierung sind die Unternehmen hingegen weitgehend indifferent. In Bezug auf das Serviceniveau ist eine leichte Bevorzugung interner Systeme festzustellen. Lediglich der Wunsch nach einem mehrsprachigen Service macht die Entscheidung für ein externes System wahrscheinlicher.

d. Unternehmensgrösse

(1) Hypothesen

Die Grösse eines Unternehmens ist ein essenzielles Kriterium, welches in der EU über die Pflicht zur Implementierung eines Meldesystems entscheidet. Das Argument, die gesetzliche Pflicht auf grosse Unternehmen (ab 250 Mitarbeitende) zu beschränken, dürfte in der Erwartung bestehen, dass diese eher in der Lage sind, die damit verbundenen Kosten tragen zu können. Die Hypothesen 5 und 6 nehmen Bezug auf diese Erwartung.

Hypothese 5: Grosse Unternehmen sind weniger kostensensibel (als KMUs) und bevorzugen externe Meldesysteme.

Hypothese 6: Grosse Unternehmen haben mit grösserer Wahrscheinlichkeit als KMUs Hinweisgebersysteme bereits implementiert.

(2) Plausibilitätstest

Die Hypothese 5, dass Grossunternehmen weniger kostensensibel sind als KMUs und ausserdem interne Meldesysteme bevorzugen, kann mit der Nullhypothese, dass (i) die entsprechenden Präferenzen unabhängig von der Betriebsgrösse sind (gemessen an der Anzahl Mitarbeiter) gegen die Alternativhypothese, dass (ii) es ein Zusammenhang besteht, getestet werden.

Kriterien: Hierzu wurden Daten zu folgenden Kriterien erhoben:

- Präferenz interner vs. externer Dienstleister
- Kostenintensität der Meldekanäle
- Einfachheit von Meldesystemen
- Anonymität des Hinweisgebers

Um Hypothese 6 auf ihre Plausibilität hin zu überprüfen, wurde die Unternehmensgrösse (gemessen an der Anzahl Mitarbeitender) in Bezug auf folgenden Kriterien überprüft:

- Vorhandensein eines Hinweisgebersystems

Fragen: Die Hypothesen 5 und 6 wurde anhand folgender Fragestellungen auf ihre Richtigkeit hin überprüft:

- «Wie viele Mitarbeitende hatte Ihr Unternehmen per 31.10.2021»?

- «Welche Bedeutung haben für Sie die folgenden Eigenschaften (Kosten, Einfachheit, Anonymität) bei der Beschaffung eines Hinweisgeberschutzsystems?»?
- «Bevorzugen Sie ein Hinweisgeberschutzsystem betriebsintern aufzubauen oder einen externen Dienstleister?»?

(3) Erkenntnisse

Die folgende Tabelle zeigt den Zusammenhang zwischen der Unternehmensgrösse und Vorhandensein eines Meldesystems. Die Hypothese, dass die Unternehmensgrösse keine Rolle spielt, dass es also keinen Zusammenhang zwischen Grösse und Existenz eines Meldesystems gibt, kann abgelehnt werden (p -Wert = 0).

| | | Hinweisgebersystem vorhanden? | | |
|--|----------------------|-------------------------------|-------|--------|
| | | ja | nein | |
| Wie viele Mitarbeitende hatte Ihr Unternehmen per 31.10.2021? | | | | |
| <i>N=144</i> | 1 - 49 | 4.2% | 18.1% | |
| <i>p-Wert=0</i> | 50 - 249 | 5.6% | 14.6% | |
| | 250 oder mehr | 38.2% | 19.4% | |
| | | 47.9% | 52.1% | 100.0% |

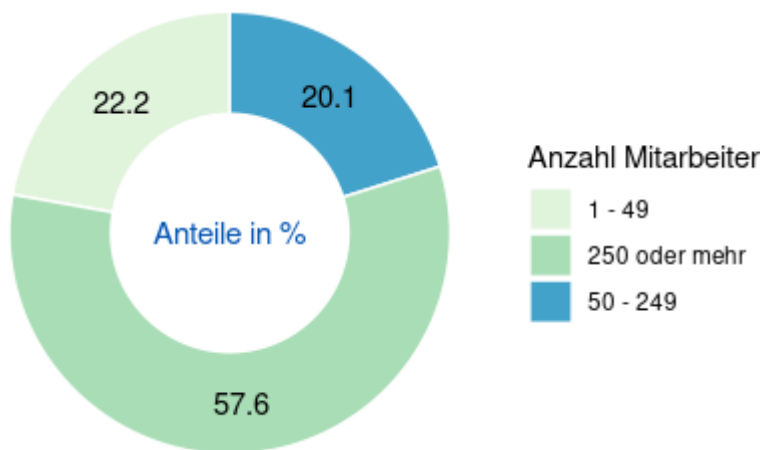


Diagramm 1: Anzahl Mitarbeitende per 31.10.2021

Wie die obenstehende Übersicht darlegt, beträgt der Anteil grosser Unternehmen mit Meldesystem 38.2 Prozent, wohingegen nur etwa halb so viele Grossunternehmen ohne Meldesystem vertreten sind. Eine eingehendere Analyse der Antworten zeigt allerdings, dass diese 19.4 Prozent nicht ausschliesslich Grossunternehmen, welche exklusiv in der Schweiz,

respektive nicht in der EU tätig sind, abbilden: Betrachtet man alle Grossunternehmen mit Tätigkeit in der EU, dann haben fast 1/3 von ihnen zum Zeitpunkt der Befragung noch keine Meldesysteme installiert. Von allen grossen, rein schweizerischen Unternehmen sind es mit ca. 40 Prozent erwartungsgemäss mehr, da für diese die gesetzliche Pflicht nicht greift. Grossunternehmen innerhalb der EU haben noch entsprechend Nachholbedarf.

Nachfolgende Tabelle zeigt auf, dass bezüglich der Entscheidung zwischen internen und externen Systemen die Unternehmensgrösse keine Rolle spielt. Unabhängig von der Anzahl der Mitarbeitenden berichten die Umfrageteilnehmer von einer leichten Vorliebe für interne Meldesysteme. Allerdings ist dieser Unterschied statistisch nicht signifikant (p-Wert=0.964).

| <u>Intern versus extern x Anzahl Mitarbeiter</u> | | | | |
|--|---------------|---------------------------|-----------------|----------------------|
| | | Anzahl Mitarbeiter | | |
| | | 1 - 49 | 50 - 249 | 250 oder mehr |
| Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister? | | | | |
| p-Wert=0.964 | intern | 58.1% | 58.6% | 56.1% |
| | extern | 41.9% | 41.4% | 43.9% |
| | N | 31 | 29 | 82 |

Die Unternehmensgrösse ist hingegen für die bevorzugten Eigenschaften (Kosten, Einfachheit der Einbindung, Anonymität der Hinweisgeber) von Meldesystemen von Bedeutung wie folgende Statistik zeigt:

| <u>Bedeutung Eigenschaften x Anzahl Mitarbeiter</u> | | | | |
|--|--|---------------------------|-----------------|-------------------|
| | | Anzahl Mitarbeiter | | |
| | | 1 - 49 | 50 - 249 | 250 o.mehr |
| Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems? | | | | |
| <u>Kosten</u> | | | | |

| | | | | |
|---|----------|-------|--------|--------|
| <i>unwichtig</i> | 1 | 6.7% | 7.1% | 3.7% |
| p-Wert=0.001 | 2 | 3.3% | 14.3% | 8.6% |
| | 3 | 30.0% | 32.1% | 37.0% |
| | 4 | 3.3% | 14.3% | 34.6% |
| <i>sehr wichtig</i> | 5 | 56.7% | 32.1% | 16.0% |
| | N | 30 | 28 | 81 |
| <u>Einfachheit der Prozesseinbettung</u> | | | | |
| <i>unwichtig</i> | 1 | 10.0% | 3.6% | 1.3% |
| p-Wert=0.026 | 2 | 0.0% | 7.1% | 0.0% |
| | 3 | 6.7% | 7.1% | 11.3% |
| | 4 | 13.3% | 28.6% | 33.8% |
| <i>sehr wichtig</i> | 5 | 70.0% | 53.6% | 53.8% |
| | N | 30 | 28 | 80 |
| <u>Anonymität für den Hinweisgeber</u> | | | | |
| <i>unwichtig</i> | 1 | 19.4% | 3.4% | 0.0% |
| p-Wert=0.000 | 2 | 6.5% | 3.4% | 2.4% |
| | 3 | 16.1% | 10.3% | 3.6% |
| | 4 | 9.7% | 24.1% | 24.1% |
| <i>sehr wichtig</i> | 5 | 48.4% | 58.62% | 69.88% |
| | N | 31 | 29 | 83 |

Den Umfrageantworten zufolge sind die Kosten für KMUs (1 bis 249 Mitarbeitende) ein wesentlich wichtigeres Kriterium als für Grossunternehmen (ab 250 Mitarbeitende). Bspw. wird von fast 57 bzw. 32 Prozent dieser Kategorie der Kostenfaktor als «sehr wichtig» bezeichnet. Bei den grossen Unternehmen deklarieren lediglich 16 Prozent dieses Kriterium als «sehr wichtig».

Die Einfachheit der Einbindung in betriebliche Prozesse ist für kleine Unternehmen ebenfalls wichtiger als für grosse; jedoch ist der Unterschied zwischen den Grössen kategorien nicht

allzu stark ausgeprägt. «Sehr wichtig» wird von kleinen Betrieben zu 70 Prozent genannt, bei den mittelgrossen sowie grossen Unternehmen sind es jeweils in etwa 54 Prozent.

Spiegelbildlich dazu verhält es sich beim Kriterium «Anonymität für den Hinweisgeber»: Hier sind es die grossen Unternehmen, die explizit mehr Wert darauflegen.

(4) Würdigung

Dass gerade kleine Unternehmen weniger Wert auf Anonymität legen als mittelgrosse bzw. grosse Unternehmen steht vermutlich im Zusammenhang, dass Kleinunternehmen oft als Familienbetrieb geführt werden, bei welchen Anonymität ohnehin kaum oder nicht gewährleistet werden kann und Hinweise auf Fehlverhalten unmittelbar persönliche Beziehungen statt Beziehungen zwischen Funktionsträgern betrifft.

Zusammenfassend erscheinen grosse Unternehmen – wie erwartet – aufgrund ihrer höheren finanziellen Ressourcen weniger sensibel bezüglich der Kosten zu sein als KMUs. Eine Vorliebe für externe Meldesysteme lässt sich bei ihnen jedoch nicht beobachten, so dass die Hypothese 5 nur teilweise bestätigt werden kann. Hingegen kann die Hypothese 6, dass grössere Unternehmen mit einer höheren Wahrscheinlichkeit Hinweisgebersysteme bereits implementiert haben, eindeutig verifiziert werden. Neben den bereits angesprochenen finanziellen Ressourcen kann dieser Umstand am besten damit erklärt werden, dass Grossunternehmen häufig über eigene in-house Complianceverantwortliche und interne Rechtsabteilungen verfügen, welche entsprechende «Compliance-Trends» antizipieren und gesetzlichen Verpflichtungen – teilweise noch vor in Kraft treten der normativen Regulierung – proaktiv zuvorkommen.

e. Schweizer Unternehmen

Die Whistleblowing-Richtlinie gilt nur für Unternehmen mit Tätigkeit in der EU. Folglich kann davon ausgegangen werden, dass Unternehmen, die ausschliesslich in der Schweiz aktiv sind, von anderen Motiven zur Einführung von Hinweisgebersystemen angetrieben werden und auch andere Präferenzmuster im Zusammenhang mit der Einrichtung derselben haben. Die folgenden Hypothesen 7 und 8 greifen diese Vermutungen wie folgt auf:

(1) Hypothesen:

Hypothese 7: Schweizer Unternehmen (ohne Aktivitäten in der EU) bevorzugen externe Meldesysteme und haben andere Ansprüche an das Serviceniveau und die Ausgestaltung (Meldekanäle) als solche mit Aktivitäten in der EU.

Hypothese 8: Schweizer Unternehmen (ohne Aktivitäten in der EU) richten Hinweisgebersysteme später ein als andere Unternehmen (mit Aktivitäten in der EU), da für sie keine gesetzliche Pflicht dazu besteht.

(2) Plausibilitätstest:

Um die Hypothesen zu evaluieren, wurde zunächst aus den Antworten eine neue Variable erstellt, die alle Unternehmen erfasst, welche ausschliesslich in der Schweiz tätig sind. Dazu wurden die Antworten aller Teilnehmenden, die auf die Frage «In welchen Ländern hat Ihr Unternehmen Betriebsstätten?», mit «Schweiz» geantwortet haben mit all jenen kombiniert, welche die übrigen Optionen verneinten. Diese neue Variable wird im Folgenden als abgeleitete Antwortoption «nur in der Schweiz» bezeichnet.

Kriterien: Diese neue Option «nur in der Schweiz» wurde mit den Antworten aus dem Fragebogen verglichen und in ein Verhältnis mit Unternehmen aus den anderen Ländern bzw. Ländergruppen gebracht. Dabei wurden folgende Kriterien analysiert;

- Zeitpunkt der Implementierung eines Hinweisgeberschutzsystems
- Präferenz interner vs. externer Dienstleister
- Bevorzugte Meldekanäle
- Prädilektion bzgl. diverser Serviceleistungen
- Präferenz interne vs. externe Dienstleister

Fragen: Es wurden folgende Fragen für rein schweizerische Unternehmen untersucht:

- «In welchen Ländern hat Ihr Unternehmen Betriebsstätten?»
- «In welchem Jahr planen Sie die Implementierung eines Hinweisgeberschutzsystems?»
- «Welches Serviceniveau ist Ihnen wichtig?»
- «Welche Meldekanäle sind Ihnen wichtig?»
- «Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister?»

(3) Erkenntnisse

Insgesamt sind 51 Teilnehmer der Umfrage «nur in der Schweiz» tätig. Diese Unternehmen sind durchschnittlich kleiner als die übrigen Teilnehmenden. Gemäss den Umfrageergebnissen haben in etwa die Hälfte aller Umfrageteilnehmer bereits Meldesysteme installiert. Die übrigen Unternehmen planen die Einführung in den kommenden Jahren, wobei Konzerne, die lediglich in der Schweiz Betriebsstätten haben, bedächtiger agieren. So planen über 2/3 von Ihnen die Einführung «2025 oder später», womit sie sich statistisch deutlich von

den anderen Ländern bzw. Ländergruppen unterscheiden. Besonders früh (69 Prozent bereits 2022) führen demzufolge all jene Unternehmen Hinweisgebersysteme ein, die «sonstige EU-Länder» als Ort ihrer Betriebsstätten angegeben haben. Deutsche, österreichische und andere EU-Unternehmen wollen diese mehrheitlich in den kommenden beiden Jahren einführen. Die dargelegten Erkenntnisse sind nachfolgender Tabelle entnehmbar:

| Land der Tätigkeit x Jahr der Einführung Hinweisgebersystem | | | | | | |
|---|---|-------------|-------------|-----------------------|----------|---------------|
| | <i>In welchem Jahr planen Sie die Implementierung eines Hinweisgeberschutzsystems?</i> | | | | | |
| | 2022 | 2023 | 2024 | 2025 o. später | | |
| <i>In welchen Ländern hat Ihr Unternehmen Betriebsstätten?</i> | | | | | N | p-Wert |
| <i>Schweiz</i> | 29.2% | 12.5% | 6.3% | 52.1% | 48 | 0.657 |
| <i>Deutschland</i> | 46.7% | 16.7% | 6.7% | 30.0% | 30 | 0.074 |
| <i>Österreich</i> | 50.0% | 12.5% | 25.0% | 12.5% | 8 | 0.068 |
| <i>sonstige EU-Länder</i> | 69.2% | 15.4% | 15.4% | 0.0% | 13 | 0.001 |
| <i>Länder ausserhalb EU</i> | 46.7% | 13.3% | 13.3% | 26.7% | 15 | 0.28 |
| <i>nur in der Schweiz</i> | 13.3% | 13.3% | 6.7% | 66.7% | 30 | 0.016 |

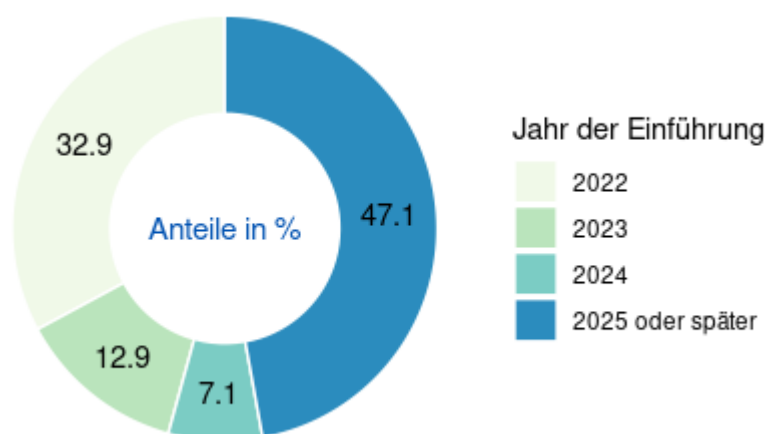


Diagramm 2: (geplantes) Jahr der Einführung eines Hinweisgeberschutzsystems

Die nachfolgenden zwei Statistiken behandeln das Serviceniveau und die Meldekanäle in Bezug auf das Tätigkeitsland der Unternehmen.

Bei den Ansprüchen an die Leistungen bzw. Eigenschaften von Meldesystemen unterscheiden sich die Schweizer Unternehmen im Vergleich zu Unternehmen anderer Länder: Wie die folgenden Resultate aufzeigen, sind Schweizer Unternehmen weniger stark als die übrigen an einer DSGVO-Konformität interessiert – legen aber weitaus mehr Wert auf Ombudsstellen als möglichen Meldekanal.

Betrachtet man alle Unternehmen, welche die Schweiz als ein Land mit einer Betriebsstätte angegeben haben, d.h. alle rein Schweizer Unternehmen und Unternehmen mit einer Niederlassung in der Schweiz gemeinsam, dann zeigt sich ein weiterer Unterschied in Bezug auf die Vorliebe einer kurzen Reaktionszeit bei Meldestellen. Diese Präferenz ist auch bei den Unternehmen aus anderen Ländern sichtbar, doch die vorliegende Evidenz lässt nicht zu, von einem statistisch signifikanten Unterschied zu sprechen, so dass letztlich offen bleiben muss, ob es sich um eine Schweizer Eigenart handelt.

| <u>Serviceniveau x Land der Tätigkeit</u> | | | | | | |
|--|---|--------------|-----------|------------------|-----------------|---------------|
| | <i>In welchen Ländern hat Ihr Unternehmen Betriebsstätten?</i> | | | | | |
| | CH | D | AT | EU andere | nicht EU | nur CH |
| <i>Welches Serviceniveau ist Ihnen wichtig?</i> | | | | | | |
| <i>24h-Erreichbarkeit</i> | 18.1% | 18.5% | 12.1% | 27.9% | 27.3% | 13.7% |
| <i>kurze Reaktionszeit</i> | 76.6% | 63.1% | 66.7% | 72.1% | 77.3% | 78.4% |
| <i>Lösungen und Empfehlungen</i> | 46.8% | 46.2% | 45.5% | 44.2% | 40.9% | 47.1% |
| <i>DSGVO-Konformität</i> | 52.1% | 72.3% | 72.7% | 69.8% | 63.6% | 45.1% |
| <i>Mehrsprachigkeit</i> | 45.7% | 43.1% | 36.4% | 48.8% | 59.1% | 45.1% |

| <u>Meldekanäle x Land der Tätigkeit</u> | | | | | | |
|--|---|----------|-----------|------------------|-----------------|---------------|
| | <i>In welchen Ländern hat Ihr Unternehmen Betriebsstätten?</i> | | | | | |
| | CH | D | AT | EU andere | nicht EU | nur CH |

| Welche Meldekanäle sind Ihnen wichtig? | | | | | | |
|--|-------|-------|--------------|--------------|--------------|--------------|
| <i>E-Mail</i> | 63.9% | 46.3% | 25.0% | 35.2% | 35.2% | 33.3% |
| <i>Telefon</i> | 73.2% | 39.3% | 26.8% | 33.9% | 35.7% | 37.5% |
| <i>Intranet</i> | 66.2% | 44.6% | 15.4% | 29.2% | 27.7% | 36.9% |
| <i>Einrichtung einer Ombudsstelle für juristische Fragen</i> | 70.2% | 40.4% | 21.3% | 19.1% | 14.9% | 46.8% |
| <i>Internet</i> | 55.7% | 52.5% | 34.4% | 37.7% | 39.3% | 26.2% |

Hypothese 7 postuliert des Weiteren eine Präferenz der Schweizer Unternehmen für externe Meldesysteme. Diese Annahme kann allerdings nicht bestätigt werden, wie die folgende Übersicht zeigt.

| <u>Land der Tätigkeit x intern vs. extern</u> | | | | |
|---|---------------|---------------|----------|---------------|
| <i>Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister?</i> | | | | |
| | intern | extern | | |
| <i>In welchen Ländern hat Ihr Unternehmen Betriebsstätten?</i> | | | N | p-Wert |
| <i>CH</i> | 51.6% | 48.4% | 143 | 0.06 |
| <i>D</i> | 62.5% | 37.5% | 143 | 0.26 |
| <i>AT</i> | 51.5% | 48.5% | 143 | 0.44 |
| <i>EU andere</i> | 55.8% | 44.2% | 143 | 0.81 |
| <i>nicht EU</i> | 52.3% | 47.7% | 143 | 0.41 |
| <i>nur CH</i> | 50.0% | 50.0% | 143 | 0.19 |

(4) Würdigung

Dass Unternehmen welche «nur in der Schweiz» tätig sind, kleiner sind als die übrigen Unternehmen, dürfte darauf zurückzuführen sein, dass all jene Unternehmen mit Betriebsstätten in mehreren Ländern – und damit tendenziell grosse Unternehmen – per Konstruktion der neuen Variablen herausgefiltert wurden.

Dass Schweizer Unternehmen Meldesysteme signifikant später einführen wollen, lässt sich damit begründen, dass für diese gegenwärtigen keine gesetzliche Verpflichtung diesbezüglich besteht. Hypothese 8 kann somit bestätigt werden.

Bei der Frage, ob interne oder externe Meldesysteme bevorzugt werden, unterscheiden sich Schweizer Unternehmen nicht von den übrigen. Demzufolge sind die Vorlieben für interne bzw. externe Meldesysteme länderübergreifend weitestgehend ausgeglichen und es lässt sich statistisch in etwa eine 50:50-Aufteilung darlegen.

Schweizer Unternehmen gewichten die DSGVO-Konformität tendenziell weniger. Dies ist darauf zurückzuführen, dass es sich hierbei um eine EU-Gesetzgebung handelt und somit i.d.R. nicht direkt auf Schweizer Unternehmen anwendbar ist – insbesondere auf solche welche einer Tätigkeit «nur in der Schweiz» nachgehen.

Bei der hohen Gewichtung Schweizer Unternehmen in Bezug auf Ombudsstellen als Meldekanal dürfte es sich um eine originär schweizerische Präferenz handeln.

Es konnten zudem festgestellt werden, dass Schweizer Unternehmen kurze Reaktionszeiten bei Meldesystemen bevorzugen, doch ist die vorliegende Evidenz in diesem Fall nicht eindeutig.

Hypothese 7 kann zwar nicht hinsichtlich der Inklination von Schweizer Unternehmen zu externen Meldestellen bestätigt werden, hinsichtlich Serviceniveau und Ausgestaltung der Meldekanäle dagegen schon. Hier sind die vorstehend dargelegten Schweizer Präferenzen zu beachten.

XII. Fazit

Die Whistleblowing-Richtlinie bringt erstes Licht in den rechtlichen Nebel, welcher das Thema Hinweisgeber seit Edward Snowden jahrelange umgeben hat. Nichtsdestotrotz sind aufgrund der bisher mangelhaften nationalen Umsetzung sowie der Auslegungsbedürftigkeit der Richtlinie noch viele Fragen offen.

Viele Unternehmen haben sich noch nicht bzw. nicht hinreichend mit dem Rechtsakt beschäftigt. Hier liegt es weitestgehend an den jeweiligen Regierungen und den entsprechenden staatlichen Institutionen die Aufmerksamkeit der Unternehmen diesbezüglich zu steigern und die rechtliche Missionsarbeit voranzutreiben.

Gerade bei Unternehmen aus Drittstaaten ausserhalb der EU muss der Blick dafür geschärft werden, dass Sie bereits jetzt unmittelbar in den Anwendungsbereich der Whistleblowing-Richtlinie fallen können, oder aber, dass sie – wie voraussichtlich im Falle

der Schweiz – das EU-Recht mittels autonomen Nachvollzugs national kodifizieren und ebenfalls umsetzen werden.

Unternehmen haben zum Teil unterschiedliche Ansprüche und Präferenzen an das Serviceniveau eines Meldekanals und an die Art der Meldekanäle. Die Abweichungen hierzu werden besonders bei den Umfrageadressaten aus EU-Ländern im Verhältnis zu solchen aus der Schweiz deutlich.

Bemerkenswert ist schliesslich, dass intrinsische Motive für Unternehmen einen wichtigeren Aspekt zur Implementierung eines Meldesystems darstellen als gesetzliche Vorgaben. Proaktiv wollen Unternehmen hier entsprechende Transparenz schaffen und nicht unbedingt Zuwarten, bis sie gesetzlich zum Tätigwerden verpflichtet werden.

XIII. Annex

1. Fragebogen mit ausgewählten summarischen Ergebnissen

| | | | |
|---|--|----------------|--------------|
| 1 | Wie viele Mitarbeitende hatte Ihr Unternehmen per 31.10.2021? | | |
| | | Prozent | N=144 |
| | <i>1 - 49</i> | 22.2% | |
| | <i>50 - 249</i> | 20.1% | |
| | <i>250 oder mehr</i> | 57.6% | |
| 2 | In welchen Ländern hat Ihr Unternehmen Betriebsstätten? | | |
| | | Prozent | N |
| | <i>in der Schweiz</i> | 64.4% | 146 |
| | <i>in Deutschland</i> | 44.5% | 146 |
| | <i>in Österreich</i> | 22.6% | 146 |
| | <i>in anderen EU-Ländern</i> | 29.5% | 146 |
| | <i>in Ländern ausserhalb der EU</i> | 30.1% | 146 |

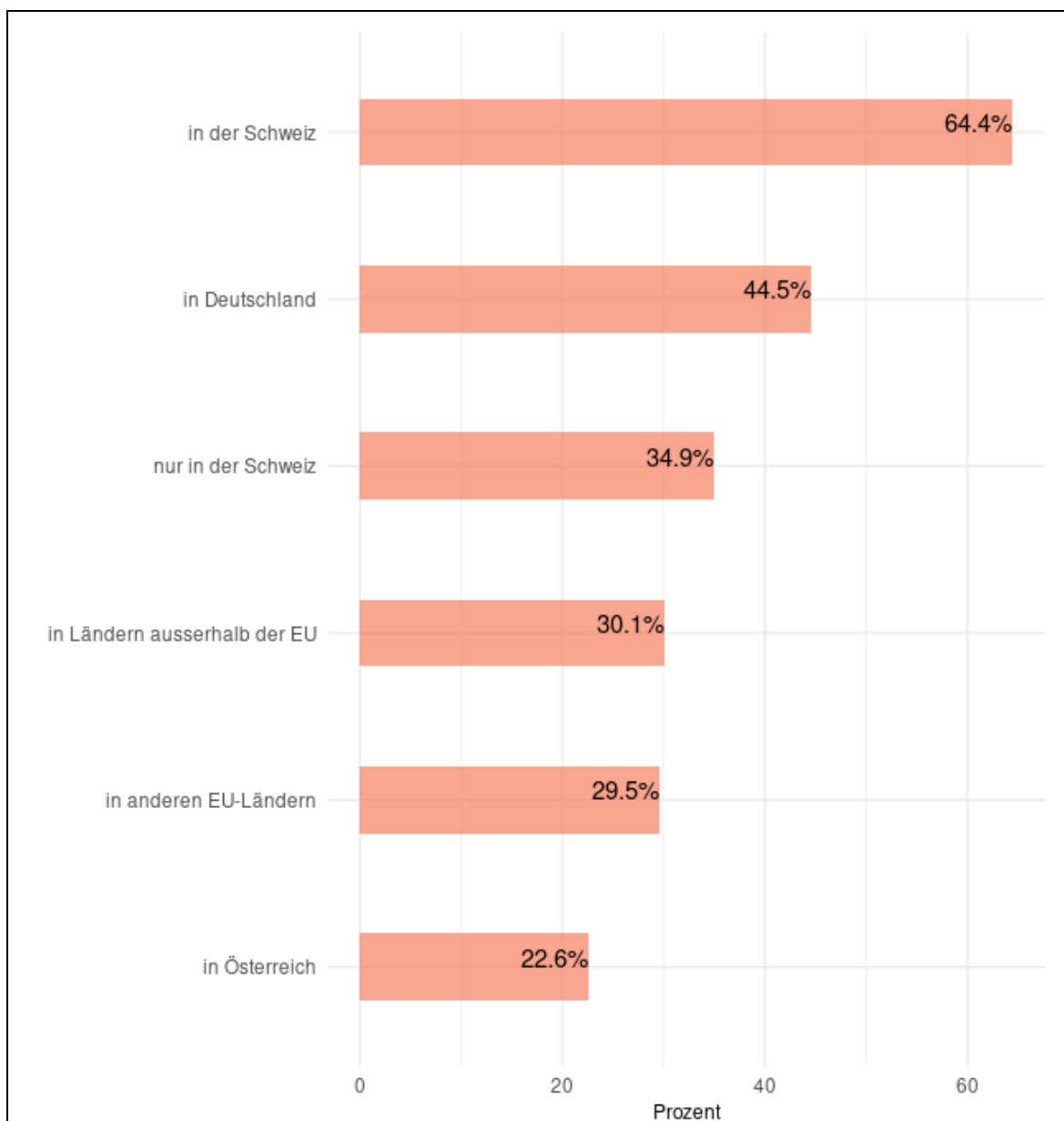


Diagramm 3: Verteilung Betriebsstätten

| | | |
|---|--|---------|
| | | |
| 3 | Wie viel Umsatz hat Ihr Unternehmen per 31.12.2020 generiert? | |
| | | |
| 4 | Der 17.12.2021 ist Stichtag für die nationale Umsetzung der EU-Richtlinie. | |
| | Verfügt Ihr Unternehmen bereits über ein Hinweisgeberschutzsystem («Whistleblower»-Schutz)? | |
| | N=146 | Prozent |

| | | | |
|---|---|----------------|------|
| | <i>ja</i> | 47.9% | |
| | <i>nein</i> | 52.1% | |
| | | | |
| 5 | In welchem Jahr planen Sie die Implementierung eines Hinweisgeberschutzsystems («Whistleblower»-Schutz)? | | |
| | | Prozent | N=70 |
| | 2022 | 32.9% | |
| | 2023 | 12.9% | |
| | 2024 | 7.1% | |
| | 2025 oder später | 47.1% | |
| | | | |
| 6 | Warum implementieren Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz)? | | |
| | | Prozent | |
| | <i>wegen einer gesetzlichen Pflicht</i> | 52.1% | |
| | <i>um Sanktionen zu verhindern</i> | 26.0% | |
| | <i>um Reputationsschäden zu vermeiden</i> | 47.3% | |
| | <i>um mit einer transparenten Unternehmenskultur für Mitarbeitende attraktiv zu sein</i> | 61.6% | |
| | <i>um die Wettbewerbsfähigkeit des Unternehmens zu steigern</i> | 17.8% | |
| | <i>andere Gründe</i> | 8.2% | |

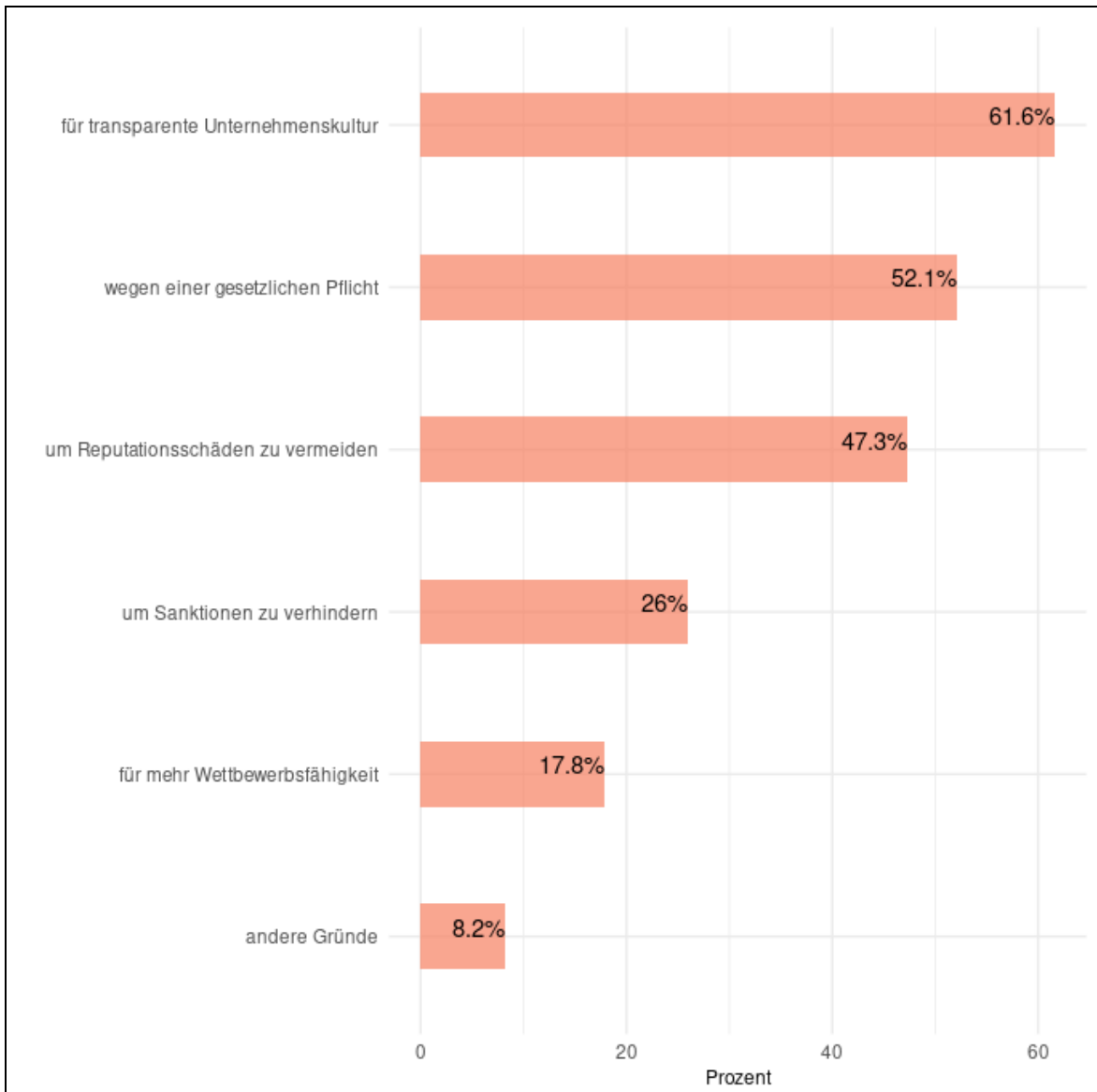


Diagramm 4: Motive für die Implementierung eines Hinweisgeberschutzsystems

| 7 | Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems («Whistleblower»-Schutz)? | | | | | |
|--|--|------|-------|---------------------|-------|-----|
| | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | N |
| | 1 | 2 | 3 | 4 | 5 | |
| <i>Kosten</i> | 5.0% | 8.6% | 35.0% | 23.6% | 27.9% | 140 |
| <i>Einfachheit der Prozesseinbettung</i> | 3.6% | 1.4% | 9.4% | 28.1% | 57.6% | 139 |
| <i>Anonymität für den Hinweisgeber</i> | 4.9% | 3.5% | 7.6% | 20.8% | 63.2% | 139 |

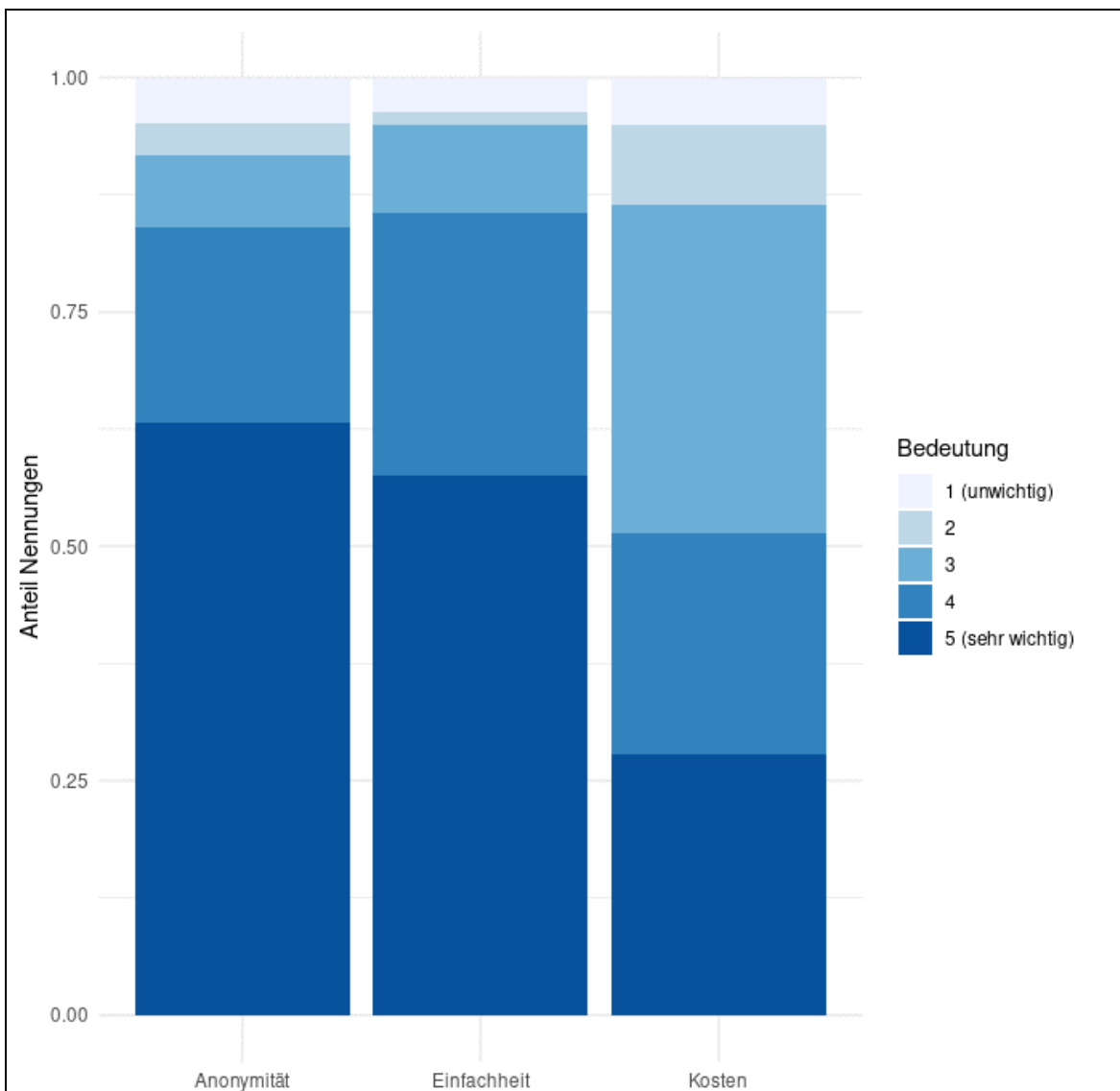


Diagramm 5: Relevanz betr. Kosten, Einfachheit und Anonymität

| | | | |
|---|--|----------------|----------|
| 8 | Welche Meldekanäle sind Ihnen wichtig? | | |
| | | Prozent | N |
| | <i>E-Mail</i> | 74.0% | 146 |
| | <i>Telefon</i> | 38.4% | 146 |
| | <i>Intranet</i> | 44.5% | 146 |
| | <i>Einrichtung einer Ombudsstelle für juristische Fragen</i> | 32.2% | 146 |
| | <i>Internet</i> | 41.8% | 146 |

| | | | |
|----|--|----------------|----------|
| | | | |
| 9 | Welches Serviceniveau ist Ihnen wichtig? | | |
| | | Prozent | N |
| | <i>24h-Erreichbarkeit</i> | 17.1% | 146 |
| | <i>kurze Reaktionszeit</i> | 70.5% | 146 |
| | <i>Lösungen und Empfehlungen</i> | 44.5% | 146 |
| | <i>DSGVO-Konformität</i> | 61.6% | 146 |
| | <i>Mehrsprachigkeit</i> | 41.8% | 146 |
| | | | |
| 10 | Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister? | | |
| | N=143 | Prozent | |
| | <i>intern</i> | 57.3% | |
| | <i>extern</i> | 42.7% | |
| | | | |
| 11 | Haben Sie weitere Anmerkungen oder Kommentare? | | |
| | | | |
| 12 | Wenn Sie Interesse haben, eine elektronische Kopie der Auswertung der Umfrage zu erhalten, geben Sie bitte hier Ihre E-Mail-Adresse an. | | |

2. Deduktive Statistiken

| | |
|---|--|
| <u>Bedeutung Eigenschaften x Meldekanäle</u> | |
| | |
| | <i>Welche Meldekanäle sind Ihnen wichtig?</i> |

| | | <i>E-Mail</i> | <i>Telefon</i> | <i>Intranet</i> | <i>Ombuds- stelle</i> | <i>Internet</i> |
|--|---------------|---------------|----------------|-----------------|---------------------------|-----------------|
| Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems? | | | | | | |
| <u>Kosten</u> | | | | | | |
| <i>unwichtig</i> | 1 | 5.7% | 5.6% | 1.6% | 4.4% | 6.8% |
| | 2 | 8.5% | 9.3% | 11.1% | 13.3% | 8.5% |
| | 3 | 36.8% | 48.1% | 42.9% | 46.7% | 28.8% |
| | 4 | 24.5% | 20.4% | 28.6% | 24.4% | 25.4% |
| <i>sehr wichtig</i> | 5 | 24.5% | 16.7% | 15.9% | 11.1% | 30.5% |
| | N | 106 | 54 | 63 | 45 | 59 |
| | p-Wert | 0.16 | 0.115 | 0.023 | 0.05 | 0.798 |
| <u>Einfachheit der Prozesseinbettung</u> | | | | | | |
| <i>unwichtig</i> | 1 | 1.9% | 3.6% | 0.0% | 2.2% | 1.7% |
| | 2 | 1.0% | 1.8% | 1.6% | 0.0% | 0.0% |
| | 3 | 9.5% | 16.1% | 7.8% | 13.3% | 5.1% |
| | 4 | 29.5% | 30.4% | 34.4% | 28.9% | 20.3% |
| <i>sehr wichtig</i> | 5 | 58.1% | 48.2% | 56.3% | 55.6% | 72.9% |
| | N | 105 | 56 | 64 | 45 | 59 |
| | p-Wert | 0.156 | 0.054 | 0.107 | 0.769 | 0.043 |

| Anonymität für den Hinweisgeber | | | | | | |
|--|---------------|-------|-------|-------|-------|-------|
| <i>unwichtig</i> | 1 | 3.7% | 1.8% | 1.5% | 0.0% | 3.3% |
| | 2 | 4.6% | 1.8% | 3.1% | 4.3% | 0.0% |
| | 3 | 8.3% | 10.7% | 3.1% | 4.3% | 9.8% |
| | 4 | 19.4% | 25.0% | 21.5% | 27.7% | 19.7% |
| <i>sehr wichtig</i> | 5 | 63.9% | 60.7% | 70.8% | 63.8% | 67.2% |
| | N | 108 | 56 | 65 | 47 | 61 |
| | p-Wert | 0.1 | 0.326 | 0.121 | 0.211 | 0.244 |

| Bedeutung Eigenschaften x Intern versus extern | | | | | | | | | |
|--|---------------|------|-------|--|----------|----------|---------------------|----------|----------|
| | | | | <i>Welche Bedeutung haben für Sie die folgenden Eigenschaften bei der Beschaffung eines Hinweisgeberschutzsystems?</i> | | | | | |
| <i>Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister?</i> | | | | | | | | | |
| | | | | <u>Kosten</u> | | | | | |
| | | | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |
| | | | | 1 | 2 | 3 | 4 | 5 | N |
| p-Wert=0 | intern | 6.2% | 7.4% | 35.8% | 24.7% | 25.9% | 81 | | |
| | extern | 3.4% | 10.3% | 34.5% | 20.7% | 31.0% | 58 | | |
| | | | | <u>Einfachheit der Prozesseinbettung</u> | | | | | |
| | | | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |

| | | 1 | 2 | 3 | 4 | 5 | N |
|--------------|---------------|---|------|-------|---------------------|-------|----|
| p-Wert=0.001 | intern | 2.5% | 2.5% | 11.4% | 25.3% | 58.2% | 79 |
| | extern | 5.1% | 0.0% | 6.8% | 32.2% | 55.9% | 59 |
| | | | | | | | |
| | | <u>Anonymität für den Hinweisgeber</u> | | | | | |
| | | <i>unwichtig</i> | | | <i>sehr wichtig</i> | | |
| | | 1 | 2 | 3 | 4 | 5 | N |
| p-Wert=0 | intern | 6.1% | 6.1% | 9.8% | 20.7% | 57.3% | 82 |
| | extern | 3.3% | 0.0% | 4.9% | 21.3% | 70.5% | 61 |

| <u>Intern versus extern x Anzahl Mitarbeiter</u> | | | | |
|---|---------------|----------------------------------|----------|---------------|
| | | <i>Anzahl Mitarbeiter</i> | | |
| | | 1 - 49 | 50 - 249 | 250 oder mehr |
| <i>Bevorzugen Sie ein Hinweisgeberschutzsystem («Whistleblower»-Schutz) betriebsintern aufzubauen oder einen externen Dienstleister?</i> | | | | |
| p-Wert=0.964 | intern | 58.1% | 58.6% | 56.1% |
| | extern | 41.9% | 41.4% | 43.9% |
| | N | 31 | 29 | 82 |

3. Anmerkungen und Kommentare

Zur Frage «Haben Sie weitere Anmerkungen oder Kommentare?», wurden folgende von den Teilnehmern folgende Antworten gegeben:

- Aktuell betrifft es unser Unternehmen noch nicht, da wir erst 12 MA beschäftigen.
- Bei der letzten Frage haben wir sowohl eine interne wie ein externe Möglichkeit - der Whistleblower kann aussuchen.
- Betrifft uns vermutlich nicht weil in DE niemand arbeitet. Best Practice Leitfaden wäre nützlich.
- Die Frage sollte eigentlich lauten, internes System oder interne Meldestelle - da hier zwei verschiedene Antworten wären. Weiters hätte auch die Frage nach dem WB System gestellt werden sollen ob eines bereits in Erarbeitung ist.
- Die Fragestellungen sind nicht gut ausgewählt. Es fehlt warum man es nicht umsetzen will
- Die Richtlinie ist für uns nicht relevant, da wir nur in der Schweiz geschäftstätig sind.
- Für ein Schweizer Unternehmen ist es komisch, hier mitzuwirken - es müsste möglich sein nicht anwendbar anzuklicken!
- Ich bin überzeugt, dass durch solche System nichts besser aber vieles schlechter wird. Es wird noch mehr unsinnige Bürokratie und Jobs aufgebaut, ohne einen Fortschritt zu erreichen.
- Ich habe den Eindruck, einen Fragebogen aus und für Deutschland auszufüllen...
- In my humble opinion, this is a weakly designed questionnaire... (I would have given the same remarks to my research methods students or thesis students preparing a quantitative study) : I'm currently the head of IT, and not the CIO, CFO or Chief leg
- Notre CP (commission du personnel) et les RH sont disponibles sans limite (Natel, SMS, courrier interne/externe, contacte directe) pour gérer les différentes remarques/insatisfactions/alertes des collaborateurs. La confidentialité est garantie par not
- Uns geht es bei der Meldestelle resp. beim Prozess nicht nur um Whistleblower, sondern um die Behandlung jeglicher Sorgen von Mitarbeitenden (Sexuelle Belästigung, Mobbing ...etc.)
- Whistleblower-System Hotline ist ein zentrales Element für die Effizienz des Compliance Management Systems. Es ist eine wesentliche Informationsquelle aus der Organisation heraus und von den Business Partnern.

- Aktuell betrifft es unser Unternehmen noch nicht, da wir erst 12 MA beschäftigen.
- Wir haben uns mit dem Thema noch nicht beschäftigt.
- Wir halten die Whistleblower-RL für zwar für notwendig, um Problemfälle aufzuzeigen, derzeit geht es aber nur in eine Richtung: der Schutz des Whistleblowers.
- Wir warten auf die Aktivitäten unserer Konzernmutter