

# Hinweisgeberrichtlinie

## Stand: November 2023

Teil 1: Einzelheiten der Richtlinie	4
Teil 2: Verfahren zur Abgabe einer Meldung	7
Teil 3: Verfahren zur Bearbeitung einer Meldung	10
Teil 4: Verbot von Repressalien	13

Diese Richtlinie gilt für die Diakonie München und Oberbayern – Innere Mission München e.V. sowie für die folgenden Tochtergesellschaften und verbundene Unternehmen:

- diakonia Dienstleistungsbetriebe GmbH der Diakonie München und Oberbayern und des Evangelisch-Lutherischen Dekanats München
- Diakonie Herzogsägmühle gGmbH
- Evangelisches Hilfswerk gGmbH
- GKP gemeinnützige Gesellschaft zur Förderung des Krisendienst Psychiatrie in Oberbayern mbH
- Hilfe im Alter gGmbH der Inneren Mission München
- HWS Hauswirtschaft und Service GmbH der Inneren Mission München
- i+s Pfaffenwinkel GmbH Gemeinnützige Integrations- und Servicegesellschaft zur Berufsförderung
- Kinderhilfe Oberland gGmbH

# Teil 1: Einzelheiten der Richtlinie

## 1. Geltungsbereich

Die Vision von Diakonie München und Oberbayern – Innere Mission München e.V. (im Folgenden als „Unternehmen“ bezeichnet) ist die Einhaltung der Unternehmensrichtlinien zu gewährleisten und eine ethische Unternehmenskultur zu fördern, indem wir bei unseren Geschäftstätigkeiten die höchsten Standards für faires Handeln, Ehrlichkeit und Integrität einhalten. Um unsere Vision zu erreichen, ist es entscheidend, dass unsere Mitarbeitenden und Partner\*innen unsere Unternehmensvision und -werte verstehen, befolgen und einhalten. Wir haben diese Richtlinien und Grundsätze eingeführt, um unsere Mitarbeiter\*innen zu ermutigen, ihre Meinung zu äußern, wenn sie Aktivitäten oder Verhaltensweisen sehen, die sie für falsch halten, um so sicherzustellen, dass wir unsere Unternehmenswerte in unserer täglichen Arbeit leben.

Das Ziel dieser Richtlinie ist es, klare Vorgaben über den Umgang von internen und externen Meldungen von Verstößen und Fehlverhalten (auch kurz „Meldungen“ oder „Hinweise“ genannt) zur Verfügung zu stellen.

Mit unserer Hinweisgeber-Richtlinie wollen wir sicherstellen, dass:

- jede\*r Mitarbeiter\*in die Möglichkeit hat, sich anonym oder vertraulich zu

äußern, wenn sie\*er das Gefühl hat, dass wir uns nicht an unsere Unternehmenswerte halten. Sie sollen einen Ort haben, an dem sie Fehlverhalten melden können, jede Meldung wird angehört und bearbeitet, und wir werden auf der Grundlage der Ergebnisse Verbesserungen vornehmen

- dass jede\*r in der Lage ist, Meldungen anonym zu erstatten. Wir verpflichten uns, die Identität von hinweisgebenden Personen zu schützen und sie müssen sich nur dann zu erkennen geben, wenn sie es wünschen
- wir jeder Meldung von Fehlverhalten nachgehen. Am Ende der Untersuchung werden wir die Ergebnisse dokumentieren und innerhalb der gesetzlichen Fristen Rückmeldung über die Folgemaßnahmen geben.

Diese Richtlinie wird allen Mitarbeitenden und leitenden Angestellten des Unternehmens bei Beginn ihres Arbeitsverhältnisses bzw. bei bestehenden Mitarbeitenden zum Zeitpunkt der Umsetzung dieser Richtlinie durch das Unternehmen zur Verfügung gestellt. Diese Richtlinie ist jedoch nicht Teil des Arbeitsvertrags. Das Unternehmen behält sich das Recht vor, diese Richtlinie jederzeit zu ändern.

## 2. Berechtigte Personen

Jede Person, die in Bezug auf das Unternehmen eine der folgenden Tätigkeiten ausübt oder ausgeübt hat, gilt als „berechtigte Person“ und fällt unter die Whistleblowing-Richtlinie des Unternehmens:

- Arbeitnehmer\*innen (*Definition Arbeitnehmer\*innen: Personen, die während eines bestimmten Zeitraums Dienstleistungen, für die sie eine Vergütung erhalten, für und unter der Leitung einer anderen Person erbringen.*)
- Arbeitnehmer\*innen in atypischen Beschäftigungsverhältnissen, einschließlich Teilzeitbeschäftigten und befristet Beschäftigten, sowie Personen, die einen Arbeitsvertrag oder ein Arbeitsverhältnis mit einem Leiharbeitsunternehmen geschlossen haben
- Freie Mitarbeitende und Selbständige, die ein Auftragsverhältnis mit dem Unternehmen haben
- Auftragnehmer einschließlich Unterauftragnehmer und Lieferanten
- Personen, die unter der Aufsicht und Leitung von Auftragnehmer\*innen, Unterauftragnehmern und Lieferant\*innen arbeiten
- Praktikant\*innen, Werkstudent\*innen und Bewerber\*innen
- Agent\*innen und Distributionsgesellschaften

- Berater\*innen, Dienstleister\*innen, Lieferant\*innen, sonstige Geschäftspartner\*innen, Prüfer\*innen
- Aufsichtsorgane, Geschäftsführer\*innen, Beiräte, Vorstände
- Menschen mit Behinderung, die in einer Werkstatt für behinderte Menschen oder bei einem anderen Leistungsanbieter nach § 60 des Neunten Buches Sozialgesetzbuch beschäftigt sind.

### 3. Meldenswerte Ereignisse

Berechtigte Personen können eine Meldung über ein Verstoß abgeben, der Folgendes darstellen könnte:

- Sexualisierte Gewalt, Diskriminierung, Mobbing
- Gewalt oder Gewaltandrohung
- Verstoß gegen die Richtlinien des Unternehmens
- Unethisches Verhalten
- Betrug, Unterschlagung, Untreue
- Korruption (aktive und passive Bestechung)
- Diebstahl
- Konsum oder Handel mit Drogen
- Sachbeschädigung

Die Liste ist nicht erschöpfend. Ereignisse jeder Art, die einen Verstoß gegen das nationale oder EU-Recht darstellen, dürfen gemeldet werden. Es ist ausreichend, einen begründeten Verdacht zu haben.

Der Begriff „Verstoß“ wird definiert als missbräuchliche Praktiken im Sinne der Rechtsprechung des Gerichtshofs, also Handlungen oder Unterlassungen, die in formaler Hinsicht nicht als rechtswidrig erscheinen, die jedoch mit dem Ziel oder Zweck der einschlägigen Rechtsvorschriften unvereinbar sind.

Sobald die Meldung abgesendet wurde, wird die berechnigte Person zu einem

„Hinweisgeber“, nachfolgend „hinweisgebende Person“, in Sinne dieser Richtlinie.

Hinweisgebende Personen können auch folgendes melden:

- Informationen, die zur Aufdeckung von bereits eingetretenen Verstößen notwendig sind
- Verstöße, die zwar noch nicht eingetreten sind, aber mit deren Eintreten mit hoher Wahrscheinlichkeit zu rechnen ist
- Handlungen oder Unterlassungen, die die hinweisgebende Person aus hinreichendem Grund als Verstöße erachtet.
- Versuche zur Verschleierung von Verstößen.

Das bösgläubige bzw. wissentliche Melden von falschen Informationen ist nicht gestattet und führt zu Sanktionen gegen die hinweisgebende Person.

Sollte Gefahr für Leib und Leben bestehen, sollte unverzüglich der Notruf 110 kontaktiert werden.

### 4. Betriebsvereinbarung

An dieser Stelle verweisen wir auf die Dienstvereinbarung, die auch im Intranet zur Verfügung steht.

## Teil 2: Verfahren zur Abgabe einer Meldung

### 1. Interne Meldestelle

Meldungen können über die „Smart Integrity Plattform“ (<https://customer-portal.smartintegrityplatform.com/DE/meldestelle-diakonie-muc-obb-120/third-party/home>) an die interne Meldestelle gesendet werden. Der Link ist unter <https://www.diakonie-muc-obb.de/meldestelle> für die Berechtigten zugänglich.

Meldungen können anonym erfolgen. Der Anbieter der Software bietet einen sicheren und anonymen Meldekanal. Wir verweisen an dieser Stelle auf Teil 2, Punkt 2.2. dieser Richtlinie.

Verantwortlich für die interne Meldestelle sind:

**Kathrin Koops**  
Rechtsabteilung Leitung Büro München  
Landshuter Allee 40, 80637 München  
T (089) 126991 118  
[kkoops@diakonie-muc-obb.de](mailto:kkoops@diakonie-muc-obb.de)

**Harald Setzwein**  
Compliance  
Von-Kahl-Str. 4, 86971 Peiting  
T (08861) 21 95 73  
[harald.setzwein@herzogsaeigmuehle.de](mailto:harald.setzwein@herzogsaeigmuehle.de)

Die Betreiberin der Smart Integrity Plattform ist die DISS-CO GmbH, Hamburg, eine Tochter der DISS-CO Ltd.

Der technische Support ist unter [support@diss-co.tech](mailto:support@diss-co.tech) zu den üblichen Geschäftszeiten (ausgenommen an Wochenenden und Feiertagen) zu erreichen.

### 2. Meldungen über die Smart Integrity Plattform

Über unsere webbasierte Plattform können Berechnigte komfortabel und sicher Hinweise an die interne Meldestelle senden. Sie haben die Möglichkeit vertraulich oder anonym zu melden. In beiden Fällen wird Ihre Identität als hinweisgebende Person geschützt.

#### 2.1. Vertrauliche Meldungen

Sie haben die Möglichkeit Meldungen vertraulich zu senden. Das bedeutet, dass Ihre Benutzerdaten an die interne Meldestelle weitergeleitet werden, sofern Sie mit einer E-Mail-Adresse eingeloggt sind. Nutzen Sie den Link auf der Webseite des Unternehmens, werden Sie bei der vertraulichen Meldung aufgefordert, Ihre Kontaktdaten anzugeben.

Wenn Sie die Option „Vertrauliches Reporting“ gewählt haben, erhalten Sie eine Benachrichtigung an die von Ihnen angegebene E-Mail-Adresse, falls ein Analyst auf der Smart Integrity Plattform eine Frage stellt. Bitte überprüfen Sie Ihren

Spam-Ordner. Es ist möglich, dass sich die Benachrichtigung dort befindet.

## 2.2. Anonyme Meldungen

Sie haben die Möglichkeit Meldungen anonym zu senden. Das bedeutet, dass Ihre Benutzerdaten (Nutzername, Kontaktdaten, IP-Adresse, Endgerät, Browserdaten) nicht an die interne Stelle weitergeleitet werden. Sie sollten so viele Details wie möglich in der Meldung aufführen. Sie können Ihrer Meldung Dateien anhängen. Die Metadaten der Dateianhänge, die Rückschlüsse auf Ihre Identität zulassen, werden automatisch von der Smart Integrity Platform entfernt. Die Dateitypen sind dabei eingeschränkt. Die üblichen Dateitypen wie MS word, excel, pdf, txt und gängige Bild- und Videodateien sind zulässig.

Sollten Sie anonym melden, berücksichtigen Sie folgendes:

- Überlegen Sie vorab, welche Personen im Unternehmen Zugriff auf die Ihnen bekannten Informationen haben, die Sie melden möchten. Damit kann der Kreis der Hinweisgeber eingegrenzt werden.
- Versuchen Sie den Sachverhalt neutral zu formulieren. Achten Sie darauf, übliche Redewendungen oder Formulierungen zu vermeiden, die Rückschlüsse auf Ihre Identität zulassen würden.

Wenn Sie anonym berichtet haben, loggen

Sie sich bitte in den ersten Wochen nach der Berichterstattung proaktiv alle zwei bis drei Tage ein, um eventuelle Fragen der Analysten zu beantworten.

## 2.3. Zugangsdaten

Sie sollten sich Ihre Zugangsdaten notieren und sicher aufbewahren. Wählen Sie immer ein sicheres Passwort mit mindestens 6 Zeichen. Sie sollten Großbuchstaben, Sonderzeichen und Zahlen kombinieren. Wenn Sie die Benutzer-ID oder das Passwort verlegen oder vergessen, reichen Sie einen identischen Bericht über die Smart Integrity Platform erneut ein und verweisen im Text auf den bereits eingereichten Bericht, möglichst unter Angabe des Datums des Berichts

## 2.4. Passwort

Das Passwort wird aus Sicherheitsgründen nicht zurückgesetzt. Wenn Sie das Passwort vergessen oder verlegt haben, reichen Sie einen identischen Bericht über die Smart Integrity Platform erneut ein und verweisen im Text auf den bereits eingereichten Bericht, möglichst unter Angabe des Datums des Berichts.

## 3. Weitere Meldewege

Sollte Gefahr für Leib und Leben bestehen, wenden Sie sich unverzüglich an den Notruf.

## 3.1. Treffen vereinbaren

Sie haben die Möglichkeit, ein Treffen für die Abgabe einer persönlichen Meldung zu vereinbaren. Nutzen Sie die Funktion „Meeting vereinbaren“ auf der Smart Integrity Platform und geben Sie einige Informationen über den Sachverhalt an. Dies hilft der internen Meldestelle, den Sachverhalt einzuordnen und eine Ansprechperson für das Treffen zu benennen. Nutzen Sie die Smart Integrity Platform, um sich über den Sachverhalt vorab auszutauschen. So bleiben die Daten im sicheren Umfeld der Plattform.

## 3.2. Externe Meldung

Wir halten unsere Mitarbeitenden an, Verstöße, die im beruflichen Kontext stehen, stets intern zu melden. Beruflicher Kontext bedeutet, dass der Sachverhalt mit der laufenden oder früheren Tätigkeit in unserem Unternehmen im Zusammenhang steht. Erhalten Hinweisgeber\*innen nach einer internen Meldung keine Rückmeldung innerhalb der gesetzlichen Frist, ist es Ihnen gestattet, extern zu melden. Die Voraussetzung hierfür ist, dass die Meldung bzw. der Verstoß, der gemeldet werden soll, vom öffentlichen Interesse ist.

Beispiele für Meldungen vom öffentlichen Interesse sind:

- Untreue des des Vorstandes oder der

Geschäftsführung, die einen erheblichen Schaden für Betroffene verursacht hat oder haben könnte

- Umweltschäden, verursacht durch Fehlentscheidungen oder Maßnahmen von Betroffenen im Unternehmen, die erhebliche Auswirkungen für die Öffentlichkeit haben oder haben könnten
- Systematische Maßnahmen, die als Betrug gegenüber Anleger\*innen, Aktionär\*innen oder Gesellschafter\*innen des Unternehmens gewertet werden könnten
- Preisabsprachen mit Wettbewerber\*innen
- Maßnahmen oder Zustände, die die physische Sicherheit von Klient\*innen und Mitarbeitenden gefährden können oder könnten verursacht hat oder haben könnte.

Sehen sich Hinweisgeber\*innen Repressalien ausgesetzt, haben sie ebenfalls die Möglichkeit extern zu melden. Eine externe Meldung ist die mündliche oder schriftliche Mitteilung von Informationen über Verstöße an die zuständigen Behörden. Welche Behörden für den Sachverhalt zuständig sind, hängt vom Inhalt der Meldung ab. In jedem Fall raten wir, dass sich Mitarbeitende, die den externen Meldeweg wählen, anwaltlichen Rat einholen sollten.

### 3.3. Externe Meldung

Hinweisgeber\*innen können für die Beschaffung, den Zugriff, die Offenlegung oder Meldung von betriebsinternen Informationen in keiner Weise haftbar gemacht werden. Für die Meldung oder Offenlegung reicht ein hinreichender Grund zu der Annahme, dass die Meldung oder Offenlegung der Information **notwendig** war, um einen Verstoß gemäß dieser Richtlinie aufzudecken.

Dies gilt, sofern die Beschaffung oder der Zugriff nicht als solche bzw. solcher eine eigenständige Straftat dargestellt hat. Im Fall, dass die Beschaffung oder der Zugriff eine eigenständige Straftat darstellt, unterliegt die strafrechtliche Haftung weiterhin dem nationalen Recht.

Beispiele sind das Hacken von Systemen, die unzulässige Verwendung von Zugängen von Kolleg\*innen zu bestimmten Systemen, Software oder anderen Applikationen, der Abzug und die Übertragung von betrieblichen Massendaten und die unerlaubte Aufnahme von Gesprächen.

## Teil 3: Verfahren zur Bearbeitung einer Meldung

### 1. Vertraulichkeit

Die interne Meldestelle prüft eingehende Meldungen im Vier-Augen-Prinzip und ist verantwortlich für die Wahrung der Vertraulichkeit der Informationen, die im Zusammenhang mit der Meldung stehen, soweit nicht nach Maßgabe von §9 HinSchG Ausnahmen vom Vertraulichkeitsgebot bestehen (z.B. in Strafsachen auf Verlangen der Strafverfolgungsbehörden).

### 2. Schutz der hinweisgebenden Person

Die interne Meldestelle ist verantwortlich für den Schutz hinweisgebenden Person, die im guten Glauben ein meldenswertes Ereignis im Sinne dieser Richtlinie über die Smart Integrity Plattform oder über andere Wege an die interne Meldestelle gemeldet hat. Die hinweisgebende Person ist vor Repressalien zu schützen. Hierzu verweisen wir auf Teil 4 dieser Richtlinie.

Hinweisgeber\*innen, die eine anonyme Meldung abgegeben haben, und die im Laufe der internen Untersuchung identifiziert wurden oder ihre Identität freiwillig offengelegt haben, sind ebenfalls zu schützen. Die interne Meldestelle ist verpflichtet, die Identität der hinweisgebenden Person in jedem Fall zu schützen.

### 3. Schutz der Betroffenen

Betroffene Personen sind natürliche oder

juristische Personen, die in der Meldung oder in der Offenlegung als eine Person bezeichnet werden, die den Verstoß begangen hat, oder mit der die bezeichnete Person verbunden sind.

*Beispiel: Es wird der Verdacht gemeldet, dass Frau Muster die falschen Stundenabrechnungen der Firma Muster GmbH wesentlich als sachlich korrekt abgezeichnet hat. Betroffene sind in diesem Fall Frau Muster und die Muster GmbH, sowie Verwandte von Frau Muster, die Mitarbeitenden und die Geschäftsführung der Muster GmbH.*

### 4. Bearbeitungsprozess

Die interne Meldestelle wird die hinweisgebende Person über die Smart Integrity Plattform innerhalb von sieben Tagen über den Eingang der Meldung benachrichtigen. Die Prüfung erfolgt im Vier-Augen-Prinzip. Der Status der Meldung wird von „Neu“ auf „Offen“ oder „Zugewiesen“ gesetzt, sobald die Meldung gelesen und verarbeitet wurde.

Hinweisgeber\*innen sind angehalten, im Laufe der internen Untersuchung zu kooperieren und Rückfragen der internen Meldestelle zeitnah und wahrheitsgemäß zu beantworten.

Innerhalb von drei Monaten nach dem Eingang der Meldung werden die

Hinweisgeber\*innen durch die interne Meldestelle über die Folgemaßnahmen informiert.

### 5. Konfliktsituation

Besteht eine Konfliktsituation in der internen Meldestelle, ist der Vorstand unverzüglich zu informieren. Die Verantwortung für die internen Untersuchungen ist an einer unabhängigen internen Person oder an einer externen Stelle zu übertragen. Der Vorstand stellt sicher, dass die Personen, die im Konflikt mit der Meldung stehen, keinen Zugriff auf die entsprechende Meldung auf der Smart Integrity Platform haben.

Besteht eine Konfliktsituation im Vorstand oder der Geschäftsführung eines verbundenen Unternehmens, sind die Eskalationsstufen unter Punkt 6. einzuhalten.

### 6. Eskalationsstufen

Die interne Meldestelle nimmt nach Erhalt der Meldungen eine erste Verifizierung des Sachverhaltes vor und stellt Rückfragen bei der hinweisgebenden Person zwecks Aufklärung. Stellen sich die gemeldeten Verdachtsmomente als korrekt oder teilweise korrekt heraus, nimmt die interne Meldestelle eine erste Risikobewertung vor. Wird das Risiko der Meldung als hoch oder sehr hoch eingestuft, ist der Vorstand

oder die Geschäftsführung des betroffenen verbundenen Unternehmen unverzüglich zu kontaktieren.

Besteht eine Beschwerdesituation innerhalb des Vorstandes oder der Geschäftsführung des betroffenen verbundenen Unternehmens, ist die interne Meldestelle befugt und verpflichtet, den jeweiligen Aufsichtsrat zu kontaktieren und über die Meldung zu informieren.

Die Konfliktsituation und die ergriffenen Maßnahmen zur Bewältigung sind im internen Kommunikationsbereich der entsprechenden Meldung auf der Smart Integrity Platform zu dokumentieren.

### 7. Externe Unterstützung

Das Unternehmen behält sich vor, für die interne Untersuchung externe Unterstützung zu beauftragen. Mit den beauftragten Personen ist eine Auftragsdatenverarbeitungsvereinbarung bzw. eine Vertraulichkeitsvereinbarung abzuschließen.

Mitarbeitende, die im Rahmen einer internen Untersuchung von der externen Unterstützung kontaktiert werden, sind zur Kooperation und wahrheitsgemäßer Auskunft zum Sachverhalt angehalten.

### 8. Herausgabe von Informationen

Die Betroffenen haben das Recht auf Information im Rahmen einer internen

Untersuchung, sofern die Meldung sie persönlich betrifft. Entsprechende Informationen können von der internen Meldestelle verschlüsselt an die Betroffenen kommuniziert werden. In bestimmten Fällen kann die interne Meldestelle die Informationen unter bestimmten Voraussetzungen zurückhalten, bis die interne Untersuchung abgeschlossen ist.

In jedem Fall ist die Identität der hinweisgebenden Person zu schützen und vertraulich zu behandeln.

### 9. Löschen von Meldungen

Die interne Meldestelle ist verpflichtet, die Meldungen DSGVO-konform zu löschen. Enthalten die Meldungen keine relevanten Informationen oder fiktive oder nicht reelle Informationen, können die Meldungen sofort nach Erhalt und Prüfung gelöscht werden.

In anderen Fällen ist wie folgt vorzugehen:

- Sobald die Aufbewahrungsfrist von 5 Jahren bzw. 3 Jahren nach Ende des Verfahrens (bei zivil-, arbeits- oder strafrechtlichen Verfahren) abgelaufen ist, setzt der Analyst die Meldung unter Angabe einer Begründung auf Löschen und ein Analyst Admin kann die Löschung bestätigen. In Ausnahmefällen kann auch eine längere

Aufbewahrungszeit begründet werden. Die Begründung ist im internen Kommunikationsbereich einzugeben.

- Sobald die Löschung bestätigt wurde, werden die Meldeinhalte sowie die Dateien, die Kommunikationsdetails extern sowie intern vollständig und unwiderruflich nach 24 Stunden gelöscht.

Der Analyst-Admin kann die Liste der gelöschten Meldungen (das Löschprotokoll) einsehen. Die folgenden Daten werden zwecks Nachverfolgung der Datenlöschungen auf unbestimmte Zeit aufbewahrt:

- Fall ID
- Meldedatum
- Kategorie
- Betreff
- Grund der Löschung
- Datum der Löschung
- Name des Analysten-Admins, der die Meldung gelöscht hat
- Name des Analyst-Admins, der die Löschung bestätigt hat

# Teil 4: Verbot von Repressalien

## 1. Definition

Repressalien sind direkte oder indirekte Handlungen oder Unterlassungen in einem beruflichen Kontext, die durch eine interne oder externe Meldung oder eine Offenlegung ausgelöst werden und durch die der hinweisgebenden Person ein ungerechtfertigter Nachteil entsteht oder entstehen kann. Dies gilt auch, wenn verbundene oder nahestehende Personen Repressalien ausgesetzt sind.

Beispiele für Repressalien:

- Kündigung von Arbeitsverträgen
- Versetzung
- Übergehung bei der Beförderung
- Zuweisung von niederen Aufgaben bzw. Aufgaben, die keinem Zusammenhang mit der bisherigen Tätigkeit stehen
- Entzug von Verantwortung
- üble Nachrede bzw. Verleumdung
- Kündigung von Verträgen bei Dienstleistern oder freien Mitarbeitenden
- Nichtverlängerung von Verträgen
- Ausschluss von Bewerbungsverfahren
- Absage bei Bewerbungen
- Setzen des Dienstleisters auf einer „schwarzen Liste“
- Nichtberücksichtigung der Bewerbung des Dienstleisters bei Ausschreibungen
- finanzielle Benachteiligung

## 2. Meldung von Repressalien

Sollten Betroffene trotz Verbot Maßnahmen gegen die hinweisgebende Person ergreifen, die als Repressalie definiert werden könnten, sind diese unverzüglich der internen Meldestelle zu melden.

Bitte verwenden Sie hierfür die Kommunikationsmöglichkeit über die Smart Integrity Plattform.

Verknüpfte Leitlinien, Prozessbeschreibungen und Richtlinien:

- Nutzungsrichtlinie der Smart Integrity Plattform
- Datenschutzrichtlinie der Smart Integrity Plattform
- Dienstvereinbarung zur Implementierung eines internen Meldekanals



## Impressum

Diakonie München und Oberbayern –  
Innere Mission München e.V.

### Compliance

Von-Kahl-Str. 4, 86971 Peiting

T (08861) 21 95 73

[meldestelle@diakonie-muc-obb.de](mailto:meldestelle@diakonie-muc-obb.de)

[www.diakonie-muc-obb.de](http://www.diakonie-muc-obb.de)