

Verfahrensordnung der Finanz Informatik GmbH & Co. KG (Finanz Informatik) für das Hinweisgebersystem gemäß Hinweisgeberschutzgesetz (HinSchG) und Beschwerdeverfahren gemäß § 8 Lieferkettensorgfaltspflichtengesetz (LkSG)

Hinweis: Die Verfahrensordnung ist im System Finanz Informatik Halo integriert und wird in diesem PDF-Dokument zusätzlich zum Download vorgehalten.

Gemäß § 8 (2) des LkSG ist eine Verfahrensordnung in Textform zugänglich zu machen. Nach der Handreichung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA) soll bei der Kommunikation und der Gestaltung der Verfahrensordnung auf die Bedürfnisse der Zielgruppen des Verfahrens eingegangen werden. Die Informationen sollen sowohl klar und übersichtlich als auch in den Sprachen aufbereitet sein, die für relevante Zielgruppen des Unternehmens wichtig sind. Die Verfahrensordnung soll an einem leicht auffindbaren Ort veröffentlicht werden (zum Beispiel auf der Website des Unternehmens, des Anbieters eines externen Beschwerdeverfahrens oder einer dafür gesondert eingerichteten Website) und möglichst ungehindert zugänglich sein.

Eine in das System des Beschwerdeverfahrens integrierte Verfahrensordnung kommt diesen Anforderungen nach. Sie ist insbesondere auch für diejenigen zugänglich, die auf Grund von Sicherheitseinstellungen der ihnen zur Verfügung stehenden IT-Umgebung gehindert sind, Dateien wie eine PDF-Datei herunterladen zu können. Auf Grund dieses Umstands hat sich die Finanz Informatik entschieden, die Verfahrensordnung direkt wie folgt in das Finanz Informatik Halo System zu integrieren:

Startseite

Integrität, Vertrauen und rechtskonformes Handeln haben für die Finanz Informatik höchste Priorität. Um mögliche Schäden im Zusammenhang mit der Geschäftstätigkeit der Finanz Informatik und damit auch bezogen auf ihre Lieferketten abwenden zu können, ist es der Finanz Informatik ein wichtiges Anliegen, von möglichen Rechtsverletzungen frühzeitig zu erfahren.

Vor diesem Hintergrund bieten wir einen unabhängigen Hinweisgebersystem-Service an, der durch Deloitte im Auftrag der Finanz Informatik für unser Haus betreut wird. Wir nennen diesen Service Finanz Informatik Halo.

Die Finanz Informatik nimmt Meldungen von Hinweisgebern über Finanz Informatik Halo sehr ernst, bearbeitet jeden eingereichten Bericht und veranlasst Untersuchungen, sofern dies möglich und erforderlich ist. Wir wollen Sie als Hinweisgeber wirksam schützen. Alle abgegebenen Meldungen sind absolut vertraulich und Sie können anonym bleiben, falls Sie nicht ausdrücklich wünschen, Ihre Identität offenzulegen.

Seite 2 von 26

Finanz Informatik Halo wurde entwickelt, um Hinweise gemäß dem deutschen Hinweisgeberschutzgesetz (HinSchG) und der zu Grunde liegenden EU-Richtlinie (EU 2019/1937) aufzunehmen.

Finanz Informatik Halo beinhaltet zudem die Funktion des Beschwerdeverfahrens nach dem Lieferkettensorgfaltspflichtengesetz und ermöglicht Personen, auf menschenrechtliche und umweltbezogene Risiken sowie auf Verletzungen menschenrechtsbezogener oder umweltbezogener Sorgfaltspflichten hinzuweisen, die durch das wirtschaftliche Handeln der Finanz Informatik im eigenen Geschäftsbereich - also bei ihr selbst - oder eines unmittelbaren oder mittelbaren Zulieferers der Finanz Informatik entstanden sind.

Finanz Informatik Halo hat verschiedene Kategorien, aus denen Sie wählen können, wenn Sie uns etwas melden möchten:

- Bestechung/Korruption/Betrug
- Gesundheit/Sicherheit/Umwelt
- Diebstahl
- Beschwerden nach dem Lieferkettensorgfaltspflichtengesetz (LkSG)
- Sonstige Verstöße gegen Unionsrecht und deutsches Recht
- Andere erhebliche Verstöße

Finanz Informatik Halo ist nicht dafür vorgesehen, beleidigende, verleumderische oder in sonstiger Weise abwertende Hinweise zum Nachteil einer Person ohne belastbare Tatsachen zu geben und ist entsprechend verantwortungsvoll zu nutzen. Sie sind daher angehalten, nur solche Informationen zu geben, von deren Richtigkeit sie nach bestem Wissen und Gewissen überzeugt sind.

Wenn Sie einen Verstoß melden wollen, dann können Sie dies [hier](#) tun.

Sie sollten zur Unterstützung der auf Ihre Meldung folgenden Maßnahmen oder Untersuchungen so viele Informationen wie möglich zur Verfügung stellen.

Hinweis zum Allgemeinen Gleichbehandlungsgesetz (AGG)

Die Verwendung der männlichen Form eines Wortes indiziert keine Benachteiligung wegen des Geschlechtes, sondern dient allein der Lesbarkeit. Selbstverständlich sind immer alle Geschlechter (m/w/d) angesprochen.

Sollten Sie weitere Fragen zu diesem Service und seiner Funktionsweise haben, dann senden Sie bitte eine E-Mail an euhalosupport@deloittece.com

Seite 3 von 26

Wie sieht der Ablauf aus?

Sie können Finanz Informatik Halo über diese Internetseite verwenden, um einen Verdacht auf einen Verstoß gegen Unionsrecht oder deutsches Recht wie Betrug, Diebstahl oder anderes Fehlverhalten zu melden. Finanz Informatik Halo ermöglicht es zudem Personen als Beschwerdeverfahren nach dem Lieferkettensorgfaltspflichtengesetz (LkSG) auf menschenrechtliche und umweltbezogene Risiken sowie auf Verletzungen menschenrechtsbezogener oder umweltbezogener Sorgfaltspflichten hinzuweisen, die durch das wirtschaftliche Handeln der Finanz Informatik im eigenen Geschäftsbereich - also bei ihr selbst - oder eines unmittelbaren oder mittelbaren Zulieferers der Finanz Informatik entstanden sind.

Die Nutzung von Finanz Informatik Halo ist vertraulich und Sie können anonym bleiben, falls Sie nicht ausdrücklich wünschen, Ihre Identität offenzulegen. Um dem von Ihnen gemeldeten Hinweis bestmöglich nachgehen zu können, sollten Sie so viele Informationen wie möglich zur Verfügung stellen.

Ein Analyst von Deloitte wird für den Finanz Informatik Halo Service die von Ihnen bereitgestellten Informationen sichten, zusammenfassen, eine konkrete Empfehlung zum weiteren Vorgehen bezüglich Ihrer Meldung geben und einen Bericht an die zuständigen Bearbeiter bei der Finanz Informatik zur weiteren Untersuchung oder Ergreifung von entsprechenden Maßnahmen senden. Die Finanz Informatik trifft dann eine Entscheidung zum weiteren Vorgehen.

Was sollte ich melden?

Wenn Sie einen Verdacht auf Fehlverhalten melden, sollten die von Ihnen bereitgestellten Informationen folgende Details beinhalten:

- Namen der beteiligten Personen
- Namen aller Zeugen (falls gegeben)
- Datum, Uhrzeit und Ort des Vorfalls bzw. der Vorfälle
- Details zu möglichen Beweisen
- Häufigkeit des Vorfalls

Zusätzlich bei Meldungen nach dem Lieferkettensorgfaltspflichtengesetz:

Zuordnung des Verstoßes

- Geschäftsbereich der Finanz Informatik – also bei ihr selbst
- bei einem unmittelbaren oder mittelbaren Zulieferer der Finanz Informatik (namentliche Nennung des Zulieferers)

Dieser Service ist vertraulich und Ihre Identität müssen Sie nicht offenlegen, falls Sie dies nicht ausdrücklich wünschen. Sie sollten zur Unterstützung darauffolgender Maßnahmen oder Untersuchungen so viele Informationen wie möglich zur Verfügung stellen.

Wie gebe ich eine Meldung ab?

Hinweisgeber-Internetseite

Sie können eine Meldung über diese Internetseite abgeben, indem Sie [hier](#) klicken.

Sie können auch Anhänge beifügen, die Sie im Zusammenhang mit Ihrer Meldung für hilfreich halten. Achten Sie dabei bitte darauf, dass diese keine Rückschlüsse auf Ihre Identität zulassen, falls Sie anonym bleiben möchten.

Telefon-Hotline für Hinweisgeber

Sie können über folgende kostenfreie Telefonnummer eine Meldung abgeben: **0800 1830529**

Sie werden mit einem Analysten von Deloitte für den Finanz Informatik Halo Service bei Deloitte verbunden, der Ihnen eine Reihe von Fragen stellen wird, um die Details zu Ihrem Verdacht zu einem Fehlverhalten in Finanz Informatik Halo aufzunehmen. Dies ist in den folgenden Sprachen möglich:

Deutsch und Englisch

Allgemeines

Dieser Service ist vertraulich und Ihre Identität müssen Sie nicht offenlegen, falls Sie dies nicht ausdrücklich wünschen. Sie sollten zur Unterstützung von darauffolgenden Maßnahmen oder Untersuchungen so viele Informationen wie möglich zur Verfügung stellen.

Häufig gestellte Fragen

Warum sollte ich Fehlverhalten melden?

Um die Finanz Informatik dabei zu unterstützen, als verlässliches, integriertes und rechtskonform handelndes Unternehmen aufzutreten, das mit seinen Mitarbeitern, Kunden und Lieferanten respekt- und vertrauensvoll umgeht und dadurch faire, sichere und integre Arbeitsplätze gewährleistet. Fehlverhalten kann einen negativen Effekt auf die Arbeitsumgebung und Reputation haben. Durch das Melden von Fehlverhalten können Sie mithelfen, z.B. durch die Aufdeckung von Betrugsfällen monetären Schäden vorzubeugen und den Mitarbeitern ein sicheres Arbeitsumfeld zu ermöglichen.

Kann ich anonym bleiben?

Sie entscheiden selbst, ob Sie anonym bleiben wollen oder nicht, wenn Sie Finanz Informatik Halo kontaktieren – Sie können Ihre Identität geheim halten oder gegenüber Finanz Informatik Halo offenlegen. Wir ermutigen Sie jedoch, Ihre Identität preiszugeben, da dies den Untersuchungs- und Aufklärungsprozess häufig erleichtert. Soweit sich Ihre Identität aus den Informationen ergeben könnte, welche Sie übermittelt haben, werden wir Maßnahmen wie z.B. die Schwärzung von Textpassagen ergreifen, damit Sie auch weiterhin anonym bleiben, falls Sie dies gewünscht haben.

Finanz Informatik Halo wird alle Informationen, die Sie zu Ihrer Person mitgeteilt haben, innerhalb von Finanz Informatik Halo vertraulich behandeln. Finanz Informatik Halo wird diese Informationen darüber hinaus nur offenlegen, wenn eine zwingende rechtliche Verpflichtung dazu besteht oder Sie im Vorfeld Ihr Einverständnis hierzu erteilt haben.

Was passiert, wenn ich eine Meldung abgebe?

Sie müssen Ihren Namen gegenüber Finanz Informatik Halo nicht nennen, wenn Sie dies nicht wollen. Ihre Meldung wird solange nur unter einer Referenznummer geführt, bis Sie sich dazu entscheiden, Ihren Namen in Finanz Informatik Halo offenzulegen.

Welche Informationen muss ich Finanz Informatik Halo geben?

Geben Sie Finanz Informatik Halo so viele Informationen wie möglich. Je mehr Informationen in Ihrer Meldung enthalten sind, umso wirkungsvoller kann Ihr Hinweis aufgegriffen und untersucht werden. Wichtige Angaben, die die weitere Bearbeitung erleichtern sind zum Beispiel:

- Namen der beteiligten Personen
- Namen aller Zeugen (falls gegeben)
- Datum, Uhrzeit und Ort des Vorfalls bzw. der Vorfälle
- Details zu möglichen Beweisen
- Häufigkeit des Vorfalls

Seite 6 von 26

Zusätzlich bei Meldungen nach dem **Lieferkettensorgfaltspflichtengesetz**:

Zuordnung des Verstoßes:

- Geschäftsbereich der Finanz Informatik – also bei ihr selbst
- bei einem unmittelbaren oder mittelbaren Zulieferer der Finanz Informatik (namentliche Nennung des Zulieferers)

Welches sind Verstöße nach dem Lieferkettensorgfaltspflichtengesetz (LkSG)?

Nach dem LkSG sind dies insbesondere Verstöße gegen die in den nachfolgend dargestellten Bereichen bestehenden Verbote:

1. **Arbeit/Arbeitsschutz:** Kinderarbeit; Zwangsarbeit und Sklaverei; unzureichender Arbeitsschutz; Beschränkung der Koalitionsfreiheit; Ungleichbehandlung im Beschäftigungsverhältnis; Vorenthalten angemessener Löhne.
2. **Schutz der Umwelt und Lebensgrundlage:** Verunreinigung von Luft, Wasser, Boden; Nutzung von Quecksilber; Verwendung von Stoffen, Chemikalien im Anwendungsbereich der Stockholm-Konvention (POP) und nicht umweltgerechter Umgang mit POP-haltigen Abfällen; Ein- und Ausfuhr gefährlicher Abfälle im Sinne des Baseler Übereinkommen; übermäßiger, die Lebensgrundlage gefährdender, Wasserverbrauch; Verletzung von Landrechten; Folter und Unterdrückung beim Einsatz von Sicherheitskräften.

Was ist, wenn ich einen Verdacht habe, mir aber nicht ganz sicher bin?

Die meisten gemeldeten Fälle werden durch die Meldungen ehrlicher Menschen aufgedeckt, die sich anfangs hinsichtlich der Faktenlage nicht ganz sicher waren. Es wird nicht von Ihnen erwartet, dass Sie jedes Detail kennen. Es reicht vollkommen aus, wenn Sie darüber berichten, was Sie wissen.

Werde ich nach der Meldung eines Vorfalls in irgendeiner Art und Weise involviert sein? Wie sind die Fristen?

Nach der Abgabe Ihrer Meldung müssen Sie sich nicht weiter damit befassen. Wenn Sie jedoch neue oder zusätzliche Informationen haben oder Änderungen an Ihrer ursprünglichen Meldung vornehmen wollen oder in den Dialog mit den zuständigen Bearbeitern Ihrer Meldung treten wollen, weil Sie z.B. Nachfragen haben, dann können Sie sich mit Ihrer Referenznummer und dem Passwort, welches Sie bei Abgabe Ihrer ursprünglichen Meldung erhalten haben, auf der Internetseite von Finanz Informatik Halo einloggen.

Der Eingang Ihrer Meldung wird innerhalb der gesetzlichen Fristen nach dem Hinweisgeberschutzgesetz (HinSchG) bzw. dem Lieferkettensorgfaltspflichtengesetz (LkSG) innerhalb von 7 Tagen bestätigt. Ebenso werden Sie über den Fortgang und Abschluss des Verfahrens -wie zuvor beschrieben- informiert. Zu einer

Seite 7 von 26

einvernehmlichen Lösungsfindung wird der zuständige Bearbeiter bedarfsweise mit Ihnen, wenn Sie dies wünschen und keine anonyme Meldung erfolgt ist, weitere Maßnahmen erörtern. Vorgänge werden innerhalb der gesetzlich festgelegten Fristen bearbeitet und möglichst abgeschlossen. In der Regel geschieht dies innerhalb von 3 Monaten nach Eingang der Meldung. Zumindest erfolgt innerhalb dieser Frist eine Rückmeldung über geplante bzw. ergriffene Maßnahmen.

Wie schnell wird Finanz Informatik nach Abgabe einer Meldung informiert?

Finanz Informatik Halo wird die zuständigen Bearbeiter bei der Finanz Informatik innerhalb von einem Werktag über Ihre Meldung informieren. Natürlich wird Finanz Informatik Halo bei sehr zeitkritischen Meldungen die Finanz Informatik unverzüglich informieren.

Bekomme ich eine Belohnung für die Meldung von Fehlverhalten?

Nein, für die Meldung von Fehlverhalten an Finanz Informatik Halo gibt es keine Belohnung.

Wie oft kann ich Finanz Informatik Halo kontaktieren?

Sie können Finanz Informatik Halo zur Meldung eines Verdachts von Fehlverhalten so oft kontaktieren wie Sie möchten.

Werden Strafverfolgungsbehörden über Meldungen an Finanz Informatik Halo informiert?

Die an Finanz Informatik Halo gemeldeten Informationen werden an die zuständigen Bearbeiter der Finanz Informatik weitergeleitet. Im Rahmen von Meldungen nach dem Lieferkettensorgfaltspflichtengesetz können in der Meldung benannte unmittelbare oder mittelbare Zulieferer der Finanz Informatik in die Bearbeitung einbezogen werden. Im Einzelfall können im Rahmen der Untersuchungen auch die entsprechenden Strafverfolgungsbehörden durch die Finanz Informatik informiert werden.

Wird es nach der Meldung zu einem Untersuchungsverfahren kommen?

Ob es zu einer Untersuchung kommt oder nicht, hängt von verschiedenen Faktoren ab, wie zum Beispiel von den bereitgestellten Informationen, den Details, der Dokumentation des Vorgangs. Die Finanz Informatik entscheidet nach Erhalt der Meldung über die erforderlichen Maßnahmen.

Wie werde ich als Hinweisgeber geschützt?

Hinweisgeber haben die Möglichkeit, ihre Hinweise in Finanz Informatik Halo komplett anonym, vertraulich (eingeschränkt anonym, d.h. nur Deloitte erfährt Ihre Identität) oder vertraulich, aber nicht anonym abzugeben. Hinweisgeber müssen somit ihre Identität nicht offenlegen, sofern sie dies nicht ausdrücklich wünschen. Darüber hinaus sind Hinweisgeber vor möglichen Nachteilen (Repressalien) im Zusammenhang mit

Seite 8 von 26

Ihren Hinweisen gemäß den Bestimmungen des Hinweisgeberschutzgesetzes (HinSchG) und des Lieferkettensorgfaltspflichtengesetzes (LkSG) geschützt – auch wenn sie ihre Identität gegenüber der Finanz Informatik offenlegen. Das gilt auch, wenn sich ein begründeter Verdacht nicht erhärtet. Es gilt nicht, wenn ein Hinweisgeber vorsätzlich unbegründete, beleidigende, verleumderische oder in sonstiger Weise abwertende Hinweise zum Nachteil einer Person ohne belastbare Tatsachen abgibt.

Wer bearbeitet die eingehenden Hinweise?

Hinweise werden zunächst durch erfahrene Analysten von Deloitte bewertet und anschließend in die weitere Bearbeitung durch ausgewählte, unabhängige und entsprechend qualifizierte Bearbeiter aus dem Fachbereich Recht und Compliance der Finanz Informatik übergeben.

Wie ist die Verfahrensordnung nach dem LkSG?

Zum leichteren Verständnis des Verfahrens sind die wesentlichen Inhalte direkt in Finanz Informatik Halo hinterlegt und zudem in die Rubrik häufig gestellte Fragen integriert.

Wird das Verfahren regelmäßig überprüft?

Wir überprüfen die Wirksamkeit regelmäßig, zumindest einmal jährlich, bzw. anlassbezogen.

Welche personenbezogenen Informationen sammelt Finanz Informatik Halo über mich und andere?

Wenn Sie Finanz Informatik Halo kontaktieren, dann werden Ihre personenbezogenen Daten nur dann erfasst, wenn Sie diese angeben möchten. Dies gilt auch für andere relevante Informationen bezüglich anderer Personen im Zusammenhang mit dem Vorfall.

Wie werden personenbezogene Informationen von Finanz Informatik Halo genutzt oder offengelegt?

Finanz Informatik Halo wird personenbezogene Daten nur im Rahmen der Bereitstellung dieses Service Ihnen und der Finanz Informatik gegenüber verwenden oder offenlegen. Finanz Informatik Halo legt die gesammelten Informationen gegenüber der Finanz Informatik offen, damit das Unternehmen im Hinblick auf Ihre Meldung reagieren kann im Rahmen rechtlicher oder regulatorischer Verpflichtungen. Ihre Identität wird der Finanz Informatik nur übermittelt, sofern sie nicht anonym bleiben wollen.

Datenschutzerklärung

Einleitung

Mit diesen Hinweisen möchten wir Sie über die Erhebung und Verarbeitung Ihrer personenbezogenen Daten durch den unten benannten Verantwortlichen und die Ihnen nach den datenschutzrechtlichen Bestimmungen zustehenden Rechte informieren. Im Zusammenhang der Nutzung des Hinweisgebersystems Finanz Informatik Halo können personenbezogene Daten verarbeitet werden. Angaben zu Ihrer Person fallen an, wenn Sie auf die Möglichkeit der anonymen Meldung verzichten. Angaben zu einer anderen Person, dessen Verhalten Sie beispielsweise melden oder als Zeuge benennen, können ebenfalls anfallen. Für beide Personengruppen gelten die folgenden Ausführungen, wobei durch Anwendung von rechtlichen Detailvorschriften sich Abweichungen im Einzelfall ergeben können.

Bei der Nutzung des Hinweisgebersystems Finanz Informatik Halo erfolgt die Verarbeitung von personenbezogenen Daten unter Beachtung der Europäischen Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG), der datenschutzrechtlich relevanten Bestimmungen sowie aller weiteren maßgeblichen Gesetze.

Verantwortlicher im Sinne des Datenschutzes Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO für die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit Finanz Informatik Halo ist

Finanz Informatik GmbH & Co. KG
Theodor-Heuss-Allee 90
D 60486 Frankfurt a.M.
Telefon +49 69 74329-0
E-Mail: kontakt@f-i.de

Im Folgenden „wir“, „uns“, „unser“ oder „Finanz Informatik“ genannt.

Finanz Informatik Halo wird im Auftrag von Finanz Informatik durch die Deloitte GmbH Wirtschaftsprüfungsgesellschaft, Rosenheimer Platz 4, 81669 München, betrieben.

Datenschutzbeauftragter

Sie erreichen unseren Datenschutzbeauftragten unter folgenden Kontaktdaten:

Finanz Informatik GmbH & Co. KG

z. H. Datenschutzbeauftragten
Laatzener Str. 5
30539 Hannover
Telefon: +49 511 5102-0
E-Mail: datenschutzbeauftragter@f-i.de

Seite 10 von 26

Jede betroffene Person kann sich jederzeit bei allen Fragen und Anregungen zum Datenschutz direkt an unseren Datenschutzbeauftragten wenden.

Umfang, Art und Zwecke der Verarbeitung

Finanz Informatik Halo ist ein System zur sicheren und vertraulichen Entgegennahme und Bearbeitung von Hinweisen über (mögliche) Gesetzes- oder Regelverletzungen gegenüber der Finanz Informatik. Das Abgeben von Hinweisen ist freiwillig.

Die Finanz Informatik setzt das Hinweisgebersystem aufgrund rechtlicher Anforderungen ein, auch um Ordnungsmäßigkeit von internen Abläufen sicherzustellen. Auch unterliegen wir rechtlichen Archivierungspflichten und bestimmten rechtlichen Meldepflichten an zuständige Behörden, wenn entsprechende Tatbestände erfüllt sind. In einigen Fällen werden wir prüfen, ob auch strafrechtliche Konsequenzen notwendig sind bzw. erstatten Anzeige.

Im Zusammenhang der Verfahren Compliance, Risikomanagement, Sicherheit sowie Interne Revision werden bestimmte Informationen, die nicht personenbezogen sind, bei der Risikobewertung einbezogen. Für die weitere Aufklärung des Sachverhalts sind Sonderprüfungen denkbar.

Rechtsgrundlage für die Verarbeitung

Finanz Informatik ist nach § 12 Abs. 1 Hinweisgeberschutzgesetz (HinSchG) und § 8 Abs. 1 Lieferkettensorgfaltspflichtengesetz (LkSG) in Verbindung mit Art. 6 Abs. 1 c DSGVO gesetzlich zum Betrieb eines Hinweisgebersystems verpflichtet. Alle Archivierungspflichten, rechtliche Meldungen, Einbezug in die Risikobewertungsverfahren usw. werden auf Grundlage dieser datenschutzrechtlichen Verarbeitungsvorschriften hierunter gefasst.

In den Fällen, in denen Sie uns keine anonymisierte Meldung übermitteln, erteilen Sie uns die Einwilligung (Art. 6 Abs. 1 a DSGVO).

Für Hinweise, die nicht unter das Hinweisgeberschutzgesetz oder das Lieferkettensorgfaltspflichtengesetz fallen, stützt sich Finanz Informatik auf das berechnete Interesse an der Aufdeckung von Missständen und der damit verbundenen Abwendung von Schäden und Haftungsrisiken (Art. 6 Abs. 1 f DSGVO).

Soweit ein Hinweis die Verarbeitung besonderer Kategorien personenbezogener Daten wie beispielsweise Gesundheitsdaten gemäß Art. 9 Abs. 1 DSGVO erforderlich macht, richtet sich diese Verarbeitung nach Art. 9 Abs. 2 a (Einwilligung) oder f (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) DSGVO oder, bei einer Meldung nach dem Hinweisgeberschutzgesetz, nach § 10 HinSchG.

Die Offenlegung der Identität der hinweisgebenden Person bei einer Meldung nach dem Hinweisgeberschutzgesetz richtet sich nach § 9 Abs. 1 bis 3 HinSchG. Die Offenlegung der Identität von Personen, die Gegenstand der Meldung sind, richtet sich nach § 9 Abs. 4 HinSchG.

Seite 11 von 26

Datenkategorien

In diesem Zusammenhang verarbeiten wir insbesondere folgende personenbezogene Daten:

Bei allen Hinweisen (Regelfall meldende Person bleibt anonym):

- Namen der beteiligten Personen
- Namen aller Zeugen (falls gegeben)
- Datum, Uhrzeit und Ort des Vorfalls bzw. der Vorfälle
- Details zu möglichen Beweisen
- Häufigkeit des Vorfalls
- Informationen zum Vorfall
- Informationen, ob und an wen der Vorfall bereits an das Unternehmen gemeldet wurde
- Beziehung der hinweisgebenden Person zum Unternehmen
- Informationen, die in Anlagen zum Hinweis enthalten sind (optional)

Bei vertraulichen Hinweisen darüberhinausgehend, soweit die Daten freiwillig geteilt werden:

- Name
- Abteilung
- E-Mailadresse
- Kontaktnummer
- Sonstige Informationen

Dauer der Datenspeicherung

Personenbezogene Daten werden so lange gespeichert, wie es die Aufklärung und abschließende Beurteilung erfordert oder ein berechtigtes Interesse von Finanz Informatik besteht oder dies aufgrund eines Gesetzes erforderlich ist. Danach werden diese Daten entsprechend den gesetzlichen Vorgaben gelöscht. Die Dauer der Speicherung richtet sich insbesondere nach der Schwere des Verdachts, der gemeldeten eventuellen Pflichtverletzung sowie der ergriffenen Maßnahmen.

Im Falle einer Meldung nach dem Hinweisgeberschutzgesetz sind Dokumentationen zu einem Verfahren nach § 11 Abs. 5 Hinweisgeberschutzgesetz (HinSchG) drei Jahre nach Abschluss des Verfahrens gelöscht. Sind rechtliche Meldepflichten an eine Aufsichtsbehörde erfolgt, müssen Meldeinhalte für längere Zeiträume gespeichert bleiben. Gleiches gilt, wenn Aufbewahrungspflichten wie beispielsweise bei strafrechtlichen Verfahren zu beachten sind.

Kategorien von Empfängern von Daten und Transfer in Drittländer

Im Zusammenhang mit Finanz Informatik Halo werden personenbezogene Daten, wie nachfolgend konkretisiert, ggf. auch an Dritte übermittelt. In Einzelfällen setzen wir spezialisierte Dienstleister, wie beispielsweise Prüfungsgesellschaften,

Seite 12 von 26

Sicherheitsexperten, Rechtsanwälte ein. Darüber hinaus können wir Ihre personenbezogenen Daten an weitere Empfänger übermitteln, wie etwa an Behörden, Ermittlungsbehörden, usw.

An Behörden, Gerichte oder andere Stellen

Im Zusammenhang mit der Bearbeitung von Hinweisen kann es erforderlich sein, Informationen, Arbeitsergebnisse und Unterlagen an Behörden, Gerichte oder andere öffentliche oder private Stellen (im Falle eines Auslandsbezugs auch im Ausland) zu übermitteln. Gleiches gilt für die Fälle, in denen Finanz Informatik einer gesetzlichen, behördlichen oder gerichtlichen Anordnung zur Herausgabe/Offenlegung von personenbezogenen Daten verpflichtet ist.

An Deloitte-interne Dienstleister sowie externe IT-Dienstleister

Deloitte als Auftragnehmer der Finanz Informatik nutzt im Rahmen seiner Tätigkeit in Einzelfällen weitere deutsche oder ausländische Deloitte-Netzwerkgesellschaften als netzwerkinterne IT-Dienstleister, die Leistungen des Betriebs, der Wartung und Pflege der von den Deloitte-Netzwerkgesellschaften genutzten IT-Systeme und Applikationen erbringen. Ein Einsatz dieser Gesellschaften mit Zugriffsrechten auf personenbezogene Daten erfolgt nur, wenn dies in den Auftragsvereinbarungen mit unseren Kunden vereinbart wurde oder im Einzelfall ohne Zustimmung gesetzlich zulässig ist.

Soweit ein Zugriff durch eine Netzwerkgesellschaft außerhalb des Europäischen Wirtschaftsraums erfolgt, wird ein angemessenes Datenschutzniveau durch die Verwendung von Standardvertragsklauseln der EU-Kommission im Sinne des Art. 46 Abs. 2 c DSGVO gewährleistet.

Cookies

Finanz Informatik Halo verwendet ausschließlich unbedingt erforderliche Cookies, um die Sicherheit der Plattform sicherzustellen (§ 25 Abs. 2 Nr. 2 TTDSG).

Ihre Datenschutzrechte

Sie können verschiedene Rechte im Zusammenhang mit Ihren personenbezogenen Daten geltend machen. Insbesondere haben Sie das Recht

- auf Auskunft, Art. 15 DSGVO

Sie können von Finanz Informatik grundsätzlich jederzeit Auskunft darüber verlangen, ob und welche personenbezogenen Daten über Sie bei Finanz Informatik wie verarbeitet werden bzw. gespeichert sind.

- auf Berichtigung, Art. 16 DSGVO

Seite 13 von 26

Sie können eine Berichtigung Ihrer von Finanz Informatik verarbeiteten personenbezogenen Daten oder, falls Sie der Ansicht sind, dass diese unzutreffend oder unvollständig sind, eine Korrektur dieser Daten fordern.

- auf Löschung („Recht auf Vergessenwerden“) Art. 17 DSGVO oder auf Einschränkung der Verarbeitung, Art. 18 DSGVO

Sie können die Löschung Ihrer von Finanz Informatik verarbeiteten personenbezogenen Daten oder eine Beschränkung der Art und Weise, wie Finanz Informatik diese Daten verarbeitet, fordern, soweit dieser nicht gesetzliche Pflichten entgegenstehen.

- auf Datenübertragbarkeit Art. 20 DSGVO

Sie können eine Kopie der Sie betreffenden personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten, um sie einer anderen Partei zu übermitteln (sofern die Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags erfolgt).

- **auf Widerspruch, Art. 21 DSGVO**

Sie können der Verarbeitung Ihrer personenbezogenen Daten durch Finanz Informatik unter compliance@f-i.de widersprechen. Für den Widerspruch entstehen keine anderen als die Übermittlungskosten nach den Basistarifen ihres Telekommunikationsanbieters.

- **auf Widerruf der Einwilligung**

Ihre Einwilligung in die Verarbeitung Ihrer personenbezogenen Daten können Sie jederzeit ohne Angabe von Gründen unter compliance@f-i.de widerrufen (sofern eine solche Verarbeitung auf Grundlage einer Einwilligung erfolgt). Bitte beachten Sie, dass die von Ihnen widerrufenen Einwilligung die Rechtmäßigkeit der Verarbeitung in der Vergangenheit nicht beeinflusst, sondern ihre Wirkung nur für die Zukunft entfaltet.

Bitte wenden Sie sich zur Wahrnehmung Ihrer Rechte an compliance@f-i.de.

- auf Beschwerde bei einer Datenschutzaufsichtsbehörde

Neben den vorstehend aufgezeigten Betroffenenrechten haben Sie zudem das Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten gegen das Datenschutzrecht verstößt.

Die für die Finanz Informatik zuständige Aufsichtsbehörde ist der Hessische Landesdatenschutzbeauftragte, Gustav-Stresemann-Ring 1, 65189 Wiesbaden, Telefon: +49 611 1408 – 0, E-Mail: poststelle@datenschutz.hessen.de

Letzte Änderung dieser Datenschutzhinweise am 25. September 2023.

English**Rules of Procedure of Finanz Informatik GmbH & Co. KG (Finanz Informatik) for the whistleblower system in accordance with the German Whistleblower Protection Act (HinSchG) and for the complaints procedure in accordance with § 8 of the German Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)**

Note: The rules of procedure are integrated in the Finanz Informatik Halo system and are also available for download in this PDF document.

According to § 8 (2) of the LkSG, rules of procedure must be made available in text form. According to the German BAFA guidelines, the needs of the target groups of the procedure should be considered when communicating and designing the rules of procedure. The information should be presented clearly and concisely and in the languages that are important for the company's relevant target groups. The rules of procedure should be published in an easy-to-find location (e.g. on the company's website, the provider of an external complaints procedure or a dedicated website) and should be as easily accessible as possible.

Rules of procedure integrated into the complaints procedure system meet these requirements. In particular, they are also accessible to those who are prevented from downloading files such as a PDF file due to the security settings of the IT environment available to them. Due to this circumstance, Finanz Informatik has decided to integrate the Rules of Procedure directly into the Finanz Informatik Halo system as follows:

Home

Integrity, trust and legally compliant actions have the highest priority for Finanz Informatik. In order to be able to avert possible damage in connection with Finanz Informatik's business activities and hence also in relation to its supply chains, it is important to Finanz Informatik to become aware of possible legal violations at an early stage.

Against this background we offer an independent whistleblowing service, which is managed by Deloitte on behalf of Finanz Informatik. We call this service Finanz Informatik Halo.

Finanz Informatik takes whistleblower reports via Finanz Informatik Halo very seriously, processes every report submitted and initiates investigations where possible and necessary. We want to effectively protect you as a whistleblower. All reports submitted are completely confidential and you can remain anonymous unless you expressly wish to reveal your identity.

Seite 15 von 26

Finanz Informatik Halo was designed to record information in accordance with the German Whistleblower Protection Act (HinSchG) and the underlying EU Directive (EU 2019/1937).

Finanz Informatik Halo also includes the function of the complaints procedure compliant with the Act on Corporate Due Diligence Obligations in Supply Chains. It enables individuals to point out human rights and environmental risks as well as violations of human rights-related or environmental obligations that have arisen as a result of Finanz Informatik's economic activities in its own business area - i.e. at its own premises - or those of a direct or indirect supplier of Finanz Informatik.

If you want to report an incident to us, Finanz Informatik Halo has various categories from which you can choose:

- Bribery/Corruption/Fraud
- Health/safety/environment
- Theft
- Complaints regarding the Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)
- Other violations of EU law and German law
- Other significant misconduct

Finanz Informatik Halo is not intended to be used to provide insulting, defamatory or otherwise derogatory information to the detriment of a person without reliable facts and must be used responsibly accordingly. You are therefore urged to provide only information that you believe to be true to the best of your knowledge and belief.

If you wish to report a violation, you may do so [here](#).

You should provide as much information as possible to support any action or investigation that follows your report.

Disclaimer regarding the General Equal Treatment Act (AGG)

The use of the masculine form of a word does not indicate any discrimination on the grounds of gender, but serves solely to enhance readability. Of course, all genders (m/f/d) are always addressed.

If you have any further questions about this service and how it works, please send an e-mail to euhalosupport@deloittece.com

Seite 16 von 26

What is the process like

You can use Finanz Informatik Halo through this website to report a suspected violation of Union or German law such as fraud, theft or other misconduct.

Finanz Informatik Halo also includes the function of the complaints procedure compliant with the Act on Corporate Due Diligence Obligations in Supply Chains. It enables individuals to point out human rights and environmental risks as well as violations of human rights-related or environmental obligations that have arisen as a result of Finanz Informatik's economic activities in its own business area - i.e. at its own premises - or those of a direct or indirect supplier of Finanz Informatik.

The use of Finanz Informatik Halo is completely confidential and you can remain anonymous unless you expressly wish to reveal your identity. To best investigate the tip you report, you should provide as much information as possible.

For the Finanz Informatik Halo Service, a Deloitte analyst will review the information you provide, summarize it, make a specific recommendation on how to proceed with your report, and send a report to the appropriate processor at Finanz Informatik for further investigation or taking appropriate action. Finanz Informatik will then make a decision on how to proceed.

What should I report

When reporting suspected misconduct, the information you provide should include the following details:

- Names of the individuals involved
- Names of any witnesses (if given)
- Date, time and location of the incident(s)
- Details of any evidence
- Frequency of the incident

In addition, in the case of reports under the Act on Corporate Due Diligence Obligations in Supply Chains:

Classification of the incident:

- business area of Finanz Informatik - i.e. at Finanz Informatik itself
- at a direct or indirect supplier of Finanz Informatik (naming of the supplier)

This service is confidential and you do not have to disclose your identity unless you specifically request it. You should provide as much information as possible to support subsequent actions or investigations.

Seite 17 von 26

How do I submit a report

Whistleblower-Website

You can submit a report through this website by clicking [here](#).

You can also include attachments that you think would be helpful in connection with your report. Please make sure that they do not reveal your identity if you wish to remain anonymous.

Whistleblower-Hotline:

You can submit a report via the following toll-free telephone number: **0800 1830529**

You will be connected to a Deloitte analyst for the Finanz Informatik Halo service at Deloitte who will ask you a series of questions to record the details of your suspected misconduct. This can be done in the following languages:

German and English

In General:

This service is confidential and you do not have to disclose your identity unless you specifically request it. You should provide as much information as possible to support any subsequent action or investigation.

FAQ

Why should I blow the whistle on misconduct?

To help Finanz Informatik be a reliable company that acts with integrity and in compliance with the law and treats its employees, customers and suppliers with respect and trust, thereby ensuring fair workplaces that are safe and operate with integrity. Misconduct can have a negative effect on the work environment and reputation. By reporting misconduct, you can help prevent monetary damage, for example, by uncovering fraud, and enable employees to work in a safe environment.

Can I be anonymous?

You decide whether or not you wish to remain anonymous when you contact Finanz Informatik Halo - you can keep your identity secret or disclose it to Finanz Informatik Halo. However, we encourage you to disclose your identity, as this often facilitates the investigation and clarification process. Where your identity could be inferred from the information you have provided, we will take steps such as redaction of text to ensure that you remain anonymous if you have requested this.

Finanz Informatik Halo will treat all information that you have provided about yourself confidentially within Finanz Informatik Halo. Furthermore, Finanz Informatik Halo will only disclose this information if there is a compelling legal obligation to do so or if you have given your consent in advance.

What happens when I make a call?

You are not required to provide your name to Finanz Informatik Halo unless you wish to do so. Your report will be known only by a reference number unless you choose to tell Finanz Informatik Halo your name.

What do I need to tell Finanz Informatik Halo?

Provide Finanz Informatik Halo with as much information as possible. The more information your report contains, the more effectively your report can be taken up and investigated. Important information that facilitates further processing is, for example:

- Names of the individuals involved
- Names of any witnesses (if given)
- Date, time and location of the incident(s)
- Details of any evidence
- Frequency of the incident

In addition, in the case of reports under the Act on Corporate Due Diligence Obligations in Supply Chains:

Classification of the incident:

- business area of Finanz Informatik - i.e. at Finanz Informatik itself
- at a direct or indirect supplier of Finanz Informatik (naming of the supplier)

What are violations according to the German Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)?

According to the Act on Corporate Due Diligence Obligations in Supply Chains, these are in particular violations of the prohibitions existing outlined in the following areas:

1. **Labor/employment protection:** child labor; forced labor and slavery; inadequate employment protection; restriction of freedom of association; unequal treatment in employment relationships; withholding of adequate wages.
2. **Protection of the environment and livelihood:** pollution of air, water, soil; use of mercury; use of substances, chemicals in the scope of the Stockholm Convention (POPs) and non-environmentally sound handling of waste containing POPs; import and export of hazardous waste as defined by the Basel Convention; excessive water consumption that endangers livelihood; violation of land rights; torture and repression in the use of security forces.

What if I suspect something is wrong, but I am not sure?

Most cases reported are uncovered through tips from honest people who are not sure of their facts. It is not expected you will know every detail. Reporting what you do know is enough.

Will I be involved after I report an incident? What are the deadlines?

Once you have submitted your notification, you do not need to deal with it any further. However, if you have new or additional information or wish to make changes to your original report or enter into a dialog with the person responsible for processing your report, e.g. because you have questions, you can log in to the Finanz Informatik Halo website using your reference number and the password you received when you submitted your original report.

Receipt of your report will be confirmed within the statutory deadlines under the Whistleblower Protection Act (HinSchG) or the Supply Chain Due Diligence Act (LkSG) within 7 days. You will also be informed about the progress and conclusion of the procedure as described above. In order to find an amicable solution, the responsible processor will discuss further measures with you if you wish and if no anonymous report has been made. Processes will be processed within the legally stipulated time limits and completed if possible. As a rule, this takes place within 3 months of receipt of the report. At the very least, feedback on planned or implemented measures will be provided within this period.

Seite 20 von 26

How soon will Finanz Informatik be notified after an incident is reported?

Finanz Informatik Halo will inform the responsible processor at Finanz Informatik about your report within one working day. Of course, in case of very time-critical reports, Finanz Informatik Halo will inform Finanz Informatik immediately.

Do I get a reward for reporting misconduct?

No, there is no reward for reporting misconduct to Finanz Informatik Halo.

How many times can I contact Finanz Informatik Halo?

You can contact Finanz Informatik Halo as many times as you want to report suspected misconduct.

Are law enforcement agencies notified of reports made to Finanz Informatik Halo?

The information reported to Finanz Informatik Halo is forwarded to the responsible Finanz Informatik processors. In the context of reports pursuant to the German Act on Corporate Due Diligence Obligations in Supply Chains (LkSG) direct or indirect suppliers of Finanz Informatik named in the report may be included in the handling. In individual cases, the relevant law enforcement authorities may also be informed by Finanz Informatik as part of the investigations.

Will there be an investigation process after each report is made?

Whether there is an investigation depends on a number of factors including the information provided, the details, documentation and company policy. Finanz Informatik will decide what action is required when they receive the report.

How am I protected as a whistleblower?

Whistleblowers have the option of submitting their information in Finanz Informatik Halo completely anonymously, confidentially (limited anonymity, i.e. only Deloitte will know your identity) or confidentially, but not anonymously. Whistleblowers therefore do not have to disclose their identity unless they expressly wish to do so. In addition,

Seite 21 von 26

whistleblowers are protected from possible disadvantages (reprisals) in connection with their reports in accordance with the provisions of the Whistleblower Protection Act (HinSchG) and the Supply Chain Due Diligence Act (LkSG) - even if they disclose their identity to Finanz Informatik. This also applies if a well-founded suspicion is not substantiated. It does not apply if a whistleblower deliberately submits unfounded, insulting, defamatory or otherwise derogatory information to the detriment of a person without substantiated facts.

Who processes the information received?

Reports are first evaluated by experienced Deloitte analysts and then passed on for further processing by selected, independent and appropriately qualified employees from the Legal and Compliance department of Finanz Informatik.

What are the procedural rules under the Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)?

To make the procedure easier to understand, the key content is stored directly in Finanz Informatik Halo and also integrated into the frequently asked questions section.

Is the procedure reviewed regularly?

We review its effectiveness regularly, at least once a year, or on an ad hoc basis.

What personal information will Finanz Informatik Halo collect about you or others?

When you contact Finanz Informatik Halo your personal details will only be collected should you wish to provide them, as well as any other relevant information about anyone else involved in the conduct.

How will Finanz Informatik Halo use or disclose personal information?

Finanz Informatik Halo will use or disclose personal information only in the course of providing this service to you and Finanz Informatik. Finanz Informatik Halo discloses the information it collects to Finanz Informatik so that it can respond to your report in the context of legal or regulatory obligations. Your identity will be provided to Finanz Informatik only if you do not wish to remain anonymous.

Data Privacy Notice**Preamble**

With this information we would like to inform you about the collection and processing of your personal data by the responsible person named below and the rights to you under the data protection regulations. Personal data may be processed in connection with the use of the Financial Informatik Halo signaling system. Your personal details will be given if you do not accept the possibility of anonymous reporting. Information about another person whose behavior you report or name as a witness may also be obtained. Both categories of persons are covered by the following explanations, although the application of detailed legal provisions may lead to discrepancies in individual cases.

When using the Finanz Informatik Halo signposting system, the processing of personal data is carried out in compliance with the European Data Protection Regulation (DSGVO), the Federal Data Protection Act (BDSG), the data protection regulations relevant to data protection law and all other relevant laws.

Responsible Data Controller per GDPR

The data controller as defined in Art. 4 (7) GDPR for the processing of your personal data in connection with Finanz Informatik Halo is:

Finanz Informatik GmbH & Co. KG
Theodor-Heuss-Allee 90
D 60486 Frankfurt a.M.
Tel: +49 69 74329-0
E-Mail: kontakt@f-i.de

Finanz Informatik Halo is operated on behalf of Finanz Informatik by Deloitte GmbH Wirtschaftsprüfungsgesellschaft, Rosenheimer Platz 4, 81669 Munich, Germany.

In the following, "we", "us", "our" or "Finanz Informatik".

Seite 23 von 26

Data Protection Officer

You can contact our Data Protection Officer at the following contact details:

Finanz Informatik GmbH & Co. KG
Attn. Data Protection Officer

Laatzener Str. 5
30539 Hannover
Tel: +49 511 5102-0
E-Mail: datenschutzbeauftragter@f-i.de

You may contact our data protection officer directly at any time with any questions or suggestions regarding data protection.

Scope, nature, and purposes of processing

Finanz Informatik Halo is a system for secure and confidential receipt and processing of tip-offs about (possible) violations of the law or internal rules against Finanz Informatik.

The submission of tip-offs is voluntary.

Finanz Informatik uses the information system based on legal requirements, also to ensure the regularity of internal procedures. We are also subject to legal archiving obligations and certain legal reporting obligations to competent authorities if relevant facts are fulfilled. In some cases, we will check whether criminal consequences are also necessary or report.

In the context of compliance, risk management, security and internal audit procedures, certain non-personal information shall be included in the risk assessment. Special investigations may be considered for further investigation of the facts.

Legal basis for processing

Finanz Informatik is legally required to operate a whistleblower system pursuant to § 12 (1) of the Whistleblower Protection Act (HinSchG) and § 8 (1) of the Supply Chain Due Diligence Act (LkSG) in conjunction with Art. 6 (1) c GDPR. All archiving requirements, legal reporting, inclusion in risk assessment procedures, etc. will be based on these data protection processing regulations.

In cases where you do not send us an anonymized message, you give us your consent (Art. 6 (1) f GDPR).

For tip-offs that are not covered by the Whistleblower Protection Act or the Supply Chain Due Diligence Act, Finanz Informatik relies on the legitimate interest in uncovering wrongdoing and the associated prevention of damage and liability risks (Art. 6 (1) f GDPR).

Seite 24 von 26

Insofar as a whistleblower requires the processing of special categories of personal data, such as health data pursuant to Art. 9 (1) GDPR, this processing is based on Art. 9 (2) (a) (consent) or (f) (assertion, exercise, or defense of legal claims) GDPR or, in the case of a whistleblower report pursuant to the Whistleblower Protection Act, § 10 HinSchG.

The disclosure of the identity of the person providing the information in the case of a report under the Whistleblower Protection Act is governed by § 9 (1) to (3) HinSchG. The disclosure of the identity of persons who are the subject of the report is governed by § 9 (4) HinSchG.

Data categories

In this context, we particularly process the following personal data:

For all tip-offs (whistleblower may remain anonymous):

- Names of persons involved
- Names of all witnesses (if provided)
- Date, time, and location of the incident(s)
- Details of possible evidence
- Frequency of the incident(s)
- Information about the incident
- Information on whether the incident has already been reported to the company and, if so, to whom
- Relationship of the whistleblower to the company
- Information contained in attachments to the report (optional)

In case the following data is provided on a voluntary basis:

- Name
- Department
- E-mail address
- Phone number
- Other information

Data retention

Personal data will be stored for as long as required for clarification and final assessment or if Finanz Informatik has a justified interest or this is required by law. Afterwards, this data is deleted in accordance with legal obligations. The data retention period depends on the severity of the suspicion and the reported possible breach of duty, and the measures taken.

In the case of a report under the Whistleblower Protection Act, documentation on proceedings under § 11 (5) HinSchG is deleted three years after the conclusion of the proceedings. Where legal reporting obligations have been imposed on a supervisory

Seite 25 von 26

authority, reporting content shall be retained for longer periods. The same applies if retention obligations, such as criminal proceedings, are to be observed.

Categories of data recipients and transfers to third countries

In connection with Finanz Informatik Halo, personal data, may also be transferred to third parties as specified below. In individual cases we use specialized service providers such as audit firms, security experts, lawyers. In addition, we can transfer your personal data to other recipients, such as authorities, investigative authorities, etc.

To authorities, courts, or other bodies

In connection with the processing of tip-offs, it may also be necessary to share information, work results and documents with authorities, courts or other public or private bodies (in the case of a cross-border case, data might be shared internationally). The same applies to cases in which Finanz Informatik is obligated by a legal, official, or judicial order to hand over/disclose personal data.

To Deloitte internal service providers and external IT service providers

As a service provider of Finanz Informatik, Deloitte relies on other German or international Deloitte network companies as network-internal IT service providers, which provide services for the operation, maintenance and support of IT systems and applications used by the Deloitte network companies. These companies may access personal data only if this has been agreed in contractual agreements with Deloitte's clients or is legally permissible in individual cases.

Insofar as access is provided by a network company outside the European Economic Area, an appropriate level of data protection is ensured using standard contractual clauses approved by the EU Commission as set forth in Art. 46 (2) c GDPR.

Cookies

Finanz Informatik Halo only uses necessary cookies to ensure the security of the platform (§ 25 (2) no. 2 TTDSG).

Your data protection rights

You may exercise various rights in connection with your personal data. In particular, you have the right to

- access, Art. 15 GDPR

In general, you can request information from Finanz Informatik at any time about whether and what personal data about you is being processed or stored by Finanz Informatik.

Seite 26 von 26

- rectification, Art. 16 GDPR

You may request that your personal data processed by Finanz Informatik will be updated or, if you believe it is inaccurate or incomplete, that it be corrected.

- erasure ("right to be forgotten"), Art. 17 GDPR or restriction of processing, Art. 18 GDPR

You may request the erasure of your personal data processed by Finanz Informatik or a restriction of the way in which Finanz Informatik processes such data, unless this conflicts with legal obligations.

- data portability Art. 20 GDPR

You may obtain a copy of the personal data concerning you that you have provided to us in a structured, commonly used, and machine-readable format in order to transfer it to another party (provided that the processing is based on consent or a contract).

- **right to object, Art. 21 GDPR**

You may object to the processing of your personal data by Finanz Informatik under compliance@f-i.de. The objection will not incur any costs other than the transmission costs according to your telecommunications provider.

- **to withdraw consent**

You may revoke your consent to the processing of your personal data at any time without giving reasons at compliance@f-i.de (if such processing is based on consent). Please note that the consent you revoke does not affect the lawfulness of the processing in the past but affects only future processing.

Please contact compliance@f-i.de to exercise your rights.

- to lodge a complaint with a data protection supervisory authority

In addition to the data subject rights outlined above, you also have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your personal data violates data protection law.

The regulatory authority responsible for Finanz Informatik is the Hessische Landesdatenschutzbeauftragte Gustav-Stresemann-Ring 1, 65189 Wiesbaden, Tel: +49 611 1408 – 0, E-Mail: poststelle@datenschutz.hessen.de

This privacy notice was last updated on 25. Sep.2023.