

Datenschutzhinweis

Personenbezeichnungen und personenbezogene Wörter gelten für alle Geschlechter.

Wir nehmen den Schutz von personenbezogenen Daten sehr ernst. Diese Datenschutzerklärung erläutert, welche personenbezogenen Daten wir bei der Nutzung des Hinweisgebersystems erheben und wie wir sie verwenden. Die Einhaltung der geltenden Datenschutzvorschriften stellen wir durch entsprechende technische und organisatorische Maßnahmen sicher.

1. Verantwortliche Stelle und Datenschutzbeauftragter

Die steirischen Raiffeisen-Genossenschaftsbanken und der Raiffeisenverband Steiermark (ZVR-Zahl 112880581) sind kraft Gesetzes gemeinsame Verantwortliche für die Verarbeitung personenbezogener Daten, die im Hinweisgebersystem einlangen, da alle eingehenden Meldungen vom Raiffeisenverband Steiermark (vor-)geprüft werden. Sie können sich mit Ihrem datenschutzrechtlichen Anliegen immer auch oder nur an den Raiffeisenverband Steiermark wenden:

E-Mail: datenschutz@rvstmk.at

Telefon: +43 (0)316-8084-0

Raiffeisenverband Steiermark

Raiffeisen-Platz 11

8074 Raaba-Grambach

Die allgemeine Datenschutzinformation des Raiffeisenverbands Steiermark finden Sie auf unserer Webseite [hier >>](#)

Den Datenschutzbeauftragten der steiermärkischen Raiffeisenbanken, Gerfried Schwarz, erreichen Sie unter:

E-Mail: datenschutz@rlbstmk.at

Telefon: +43 (0)316-4002-0

Raiffeisen-Landesbank Steiermark AG

Radetzkystraße 15

8010 Graz

Hinweisgeber sind hinsichtlich personenbezogener Daten, von denen sie **wissen**, dass sie über das zur Weiterverfolgung des Hinweises Erforderliche hinausgehen, Verantwortliche im Sinne der DSGVO (§ 8 Abs. 4 Z 1 HinweisgeberInnenschutzgesetz). Hinweisgeber haben sich bei der Eingabe personenbezogener Daten sohin auf jene Daten zu beschränken, die für die Weiterverfolgung des Hinweises ihrer Meinung nach erforderlich sind.

2. Welche personenbezogene Daten verarbeiten wir?

Wir können vorab nicht näher aufschlüsseln, welche personenbezogenen Daten wir über das Hinweisgebersystem erhalten werden, da das Meldeformular durch den Hinweisgeber befüllbare Textfelder enthält. Abhängig vom Inhalt der Meldung und dem Umstand, ob die Meldung anonym ist, könnten daher folgende Kategorien personenbezogener Daten verarbeitet werden:

- Personenstammdaten (natürlicher Personen: z.B. Vorname, Nachname, Organisationsdaten)
- Kommunikationsdaten (z.B. Telefon, E-Mail, Adresse)
- Für das Hinweisgebersystem: Fall-ID und Passwort

- Informationen zu (potentiellen) Straftaten oder Verdachtsmomente zu Straftaten
- Bild- und/oder Tonaufzeichnungen
- besondere Kategorien personenbezogener Daten im Sinne der DSGVO. Dazu gehören bspw. Informationen zur rassischen und/oder ethnischen Herkunft, religiösen und/oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit oder sexuellen Orientierung.
- Daten, die wir über das Hinweisgebersystem erhalten

Im Rahmen von Hinweisen kann es zur Verarbeitung personenbezogener Daten

- von Hinweisgebern (jene Personen, die Hinweise einmelden),
- von vom Hinweis betroffenen Personen (jene Personen, auf die sich Hinweise beziehen) und/oder
- von Dritten (z.B. Zeugen, Unterstützer des Hinweisgebers, von Personen, die von Folgemaßnahmen betroffen oder in diese involviert sind) kommen.

Ergänzungen in Bezug auf Hinweisgeber:

Die Nutzung des Hinweisgebersystems ist ohne die Angabe personenbezogener Daten des Hinweisgebers möglich. Hinweisgeber können jedoch im Rahmen des Hinweisgeberprozesses freiwillig ihre personenbezogene Daten bekanntgeben, insbesondere Angaben zu ihrer Identität, Vor- und Nachname, Land des Wohnsitzes, Telefonnummer oder E-Mail-Adresse.

Überdies verarbeiten wir für das sichere Postfach das vom Hinweisgeber gesetzte Passwort und die Fall-ID.

Ergänzungen in Bezug auf eine vom Hinweis betroffene Person und Dritte:

Hinweise können personenbezogene Daten der vom Hinweis betroffenen Personen und Dritter enthalten. Hinweisgeber haben sich – wie unter Punkt 1. zur verantwortlichen Stelle ausgeführt – bei der Eingabe solcher personenbezogener Daten auf jene Daten zu beschränken, die für die Weiterverfolgung des Hinweises ihrer Meinung nach erforderlich sind. Hinweisgeber sind hinsichtlich personenbezogener Daten, von denen sie **wissen**, dass sie über das zur Weiterverfolgung des Hinweises Erforderliche hinausgehen, Verantwortliche im Sinne der DSGVO (§ 8 Abs. 4 Z 1 HinweisgeberInnenschutzgesetz).

Von einem Hinweis betroffene Personen erhalten grundsätzlich die Möglichkeit, sich zu dem Hinweis zu äußern. Dies gilt dann und solange nicht, als dies die weitere Untersuchung behindern könnte. Eine Information unterbleibt auch dann, wenn diese den Schutz der Identität der Person des Hinweisgebers, seiner Unterstützer oder Personen im Umfeld des Hinweisgebers, die nachteilige Folgen aus der Hinweisgebung zu befürchten hätten, gefährdet (§ 8 Abs. 9 letzter Satz HinweisgeberInnenschutzgesetz).

3. Zweck der Verarbeitung

Zweck der vorliegenden Datenverarbeitung ist es, Personen, die eine Rechtsverletzung im Raiffeisenverband Steiermark, in den steirischen Raiffeisen-Genossenschaftsbanken oder in der Sigma Wirtschaftsprüfungs GmbH (FN 492815d; im Folgenden kurz: Sigma) wahrgenommen haben, die Meldung ihrer Wahrnehmung zu ermöglichen. So haben wir die Chance, Rechtsverletzungen früh zu erkennen, aufzuklären, abzustellen und überhaupt zu verhindern. Das liegt in unserem, aber auch im öffentlichen Interesse. Wir haben uns daher entschieden, Hinweise, die bei uns einlangen, auch dann zu prüfen, wenn sie über den

Anwendungsbereich des HinweisgeberInnenschutzgesetzes (HSchG) hinausgehen. Wir weisen ausdrücklich darauf hin, dass das HSchG den umfassenden Schutz für Hinweisgeber auf Meldungen im Anwendungsbereich des HSchG beschränkt.

Das dafür eingerichtete Hinweisgebersystem ermöglicht es Hinweisgebern, mit uns in Verbindung zu treten und Hinweise zu Compliance- und Rechtsverstößen zu melden. Wir verarbeiten personenbezogene Daten im Hinweis, um die von Hinweisgebern über das Hinweisgebersystem gemachte Meldung zu prüfen und die mutmaßlichen Compliance- und Rechtsverstöße zu untersuchen. Hierbei kann es vorkommen, dass wir Rückfragen an Hinweisgeber haben. Dafür nutzen wir die Kommunikation über das Hinweisgebersystem ("Sicheres Postfach"). Hierbei steht für uns die Vertraulichkeit der Person des Hinweisgebers sowie der von Hinweisgebern gemachten Angaben an erster Stelle.

4. Weitergabe der personenbezogenen Daten

Zur Erfüllung der oben genannten Zwecke kann es erforderlich sein, dass wir personenbezogene Daten an externe Stellen wie Anwaltskanzleien, Straf- oder Wettbewerbsbehörden übermitteln. Ohne rechtliche Notwendigkeit werden wir uns dabei nicht an externe Stellen außerhalb der Europäischen Union wenden.

Zur Fallbearbeitung kann es notwendig sein, dass der Raiffeisenverband Steiermark personenbezogene Daten an die Gesellschaft (steirische Raiffeisen-Genossenschaftsbank oder Sigma) weitergibt, in der sich der gemeldete Vorfall ereignet hat. Es wird mittels interner Datenschutzregelungen und/oder entsprechender vertraglicher Vereinbarungen ein einheitliches Datenschutzniveau sichergestellt. In sämtlichen Fällen verbleibt die Verantwortung zur Datenverarbeitung (auch) bei den oben angegebenen Verantwortlichen.

Die technische Umsetzung unseres Hinweisgebersystems erfolgt in unserem Auftrag durch die EQS Group GmbH (FN 560345m), Siebensterngasse 31/8, 1070 Wien ("**EQS**"). Personenbezogene Daten werden im für die technische Umsetzung notwendigen Umfang auch von EQS verarbeitet. Hierfür haben wir einen Auftragsverarbeitungsvertrag mit EQS abgeschlossen.

5. Rechtsgrundlagen der Verarbeitung

Es gibt mehrere Grundlagen für die Verarbeitung der in einem Hinweis enthaltenen personenbezogenen Daten (Rechtmäßigkeit der Verarbeitung):

- Betrifft der Hinweis einen Fall, der im Anwendungsbereich des HinweisgeberInnenschutzgesetzes (HSchG) liegt, stützen wir die Verarbeitung auf Art. 6 Abs. 1 lit. c und lit. e und Art. 9 Abs. 2 lit. f und g DSGVO in Verbindung mit dem HSchG.
- Banken sind systemrelevant. Rechtstreue und Regelkonformität (Compliance) von Banken stellen folglich im allgemeinen Interesse sicher, dass das Finanzsystem und die Realwirtschaft funktionieren. Für Hinweise, die steirische Raiffeisen-Genossenschaftsbanken betreffen, stützen wir die Verarbeitung daher (auch) auf Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. g DSGVO in Verbindung mit der jeweiligen Rechtsgrundlage, die Banken zur Entgegennahme des Hinweises verpflichtet (z.B. § 40 FM-GwG, § 99g BWG inklusive der weiteren Rechtsgrundlagen, die im Anhang angeführt sind). Der Raiffeisenverband Steiermark stützt sich (auch) auf seine gesetzliche Prüfpflicht als Revisionsverband (§§ 1 ff Genossenschaftsrevisionsgesetz 1997).

- Betrifft ein Hinweis Verstöße gegen das Abschlussprüfer-Aufsichtsgesetz, stützen wir unsere Verarbeitung (auch) auf Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. g DSGVO in Verbindung mit § 66 Abschlussprüfer-Aufsichtsgesetz.
- Die Verarbeitung stützen wir überdies auf die uns jeweils treffende gesetzliche Verpflichtung, rechtskonform zu handeln und Rechtsansprüche aus rechtswidrigem Verhalten zu verfolgen bzw. abzuwehren (Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. b und f DSGVO).
- Die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten iSd Art 10 DSGVO erfolgt, soweit dies für die Zweckerreichung unbedingt erforderlich und überdies durch § 4 Abs. 3 Z 2 DSG, Art. 6 Abs. 1 lit. f, Art. 9 Abs. 2 lit. f DSGVO, § 8 Abs. 6 HSchG und/oder die Normen im Anhang gerechtfertigt ist.
- Die Verarbeitung personenbezogener Daten kann überdies erfolgen, sofern dies zur Wahrung berechtigter Interessen der steirischen Raiffeisen-Genossenschaftsbanken, der Sigma oder des Raiffeisenverbands Steiermark erforderlich ist (Art. 6 Abs. 1 lit. f DSGVO). So haben wir etwa ein berechtigtes Interesse daran, Compliance- und Rechtsverletzungen in unseren Unternehmen rasch zu erkennen und zu verhindern. Dafür müssen wir Hinweisen, die zur Prävention rechtswidrigen Verhaltens beitragen, die rechtswidriges Verhalten aufdecken oder verhindern, nachgehen können.

Wir beschränken die Verarbeitung immer auf jene personenbezogenen Daten, die wir zur Wahrung der oben genannten Zwecke (Feststellung und Ahndung einer Rechtsverletzung) benötigen. Werden uns überschüssige Daten übermittelt, löschen wir diese umgehend.

Entfernen wir den Personenbezug von Daten irreversibel (Anonymisierung), können wir die anonymisierten Datensätze für statistische Zwecke verwenden. So können wir etwa auswerten und speichern, wie viele Meldungen über das Hinweisgebersystem eingegangen sind.

Wir verarbeiten Ihre personenbezogenen Daten zu keinen anderen als den oben angeführten Zwecken. Andernfalls werden wir vorher eine entsprechende Einwilligung bei Ihnen einholen.

6. Technische Umsetzung und Sicherheit Ihrer Daten

Das Hinweisgebersystem enthält eine Möglichkeit zur anonymen Kommunikation über eine verschlüsselte Verbindung. Bei der Nutzung werden IP-Adresse und derzeitiger Standort des Nutzers zu keinem Zeitpunkt gespeichert. Nach dem Absenden eines Hinweises erhält der Hinweisgeber Zugangsdaten zu seinem sicheren Postfach (Fall-ID und persönliches Passwort), um mit uns weiterhin geschützt kommunizieren zu können. Macht der Hinweisgeber im Hinweis oder in seinem Passwort keine Angaben zu seiner Person, kann der Hinweisgeber auch über die Fall-ID und das persönliche Passwort nicht identifiziert werden.

Die von Ihnen zur Verfügung gestellten Daten werden auf einer besonders gesicherten Datenbank gespeichert. Sämtliche auf der Datenbank gespeicherten Daten sind nach dem aktuellen Stand der Technik verschlüsselt.

7. Dauer der Speicherung

Personenbezogene Daten speichern wir nur so lange, wie es für die Bearbeitung eines Hinweises zu den oben angeführten Rechtmäßigkeitsgründen erforderlich ist. Eine Speicherung muss darüber hinaus erfolgen, wenn dies durch den europäischen oder nationalen Gesetzgeber zur Erfüllung gesetzlicher Verpflichtungen, wie etwa Aufbewahrungspflichten, vorgesehen ist.

Fällt der jeweilige Speicher- oder Aufbewahrungsgrund weg, werden sämtliche personenbezogenen Daten gelöscht oder anonymisiert.

Für Meldungen im Anwendungsbereich des HSchG hat der Gesetzgeber eine solche besondere Aufbewahrungspflicht normiert:

Nach § 8 Abs. 11 HSchG sind wir dazu verpflichtet, personenbezogene Daten ab ihrer letztmaligen Verarbeitung oder Übermittlung fünf Jahre und darüber hinaus so lange aufzubewahren, als es zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der StPO erforderlich ist. Nach Entfall der Aufbewahrungspflicht löschen wir personenbezogene Daten. Tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen sind zu protokollieren. Protokolldaten über diese Vorgänge sind ab ihrer letztmaligen Verarbeitung oder Übermittlung bis drei Jahre nach Entfall der fünfjährigen Aufbewahrungspflicht aufzubewahren (§ 8 Abs. 12 HSchG). Ist die Aufbewahrung über diese Fristen hinaus notwendig, um einen der oben angeführten Zwecke zu erreichen, stützen wir uns für die längere Aufbewahrung auf den Anwendungsvorrang der DSGVO vor dem HSchG.

8. Schutz der Identität

Jeder Hinweis wird im Raiffeisenverband Steiermark von eigens dafür berechtigten Mitarbeitern weisungsfrei und unbefangen bearbeitet und geprüft. Unbefangene, zuständige Mitarbeiter jener Gesellschaft (steirische Raiffeisen-Genossenschaftsbank oder Sigma), die die Meldung betrifft, werden soweit eingebunden, als dies für die Fallbearbeitung (z.B. Behebung von Rechtsverletzungen) erforderlich ist.

Von Hinweisgebern

Legt ein Hinweisgeber seine Identität offen, ist diese von den mit der Bearbeitung des Hinweises betrauten Personen zu schützen. Dies gilt auch für alle anderen Informationen, aus denen die Identität des Hinweisgebers direkt oder indirekt abgeleitet werden kann.

Die Identität von Hinweisgebern darf nur dann offengelegt werden, wenn eine Verwaltungsbehörde, ein Gericht oder die Staatsanwaltschaft dies im Rahmen des verwaltungsbehördlichen oder gerichtlichen Verfahrens oder eines Ermittlungsverfahrens nach der StPO für unerlässlich und im Hinblick auf eine Gefährdung von Hinweisgebern sowie auf die Stichtichtigkeit und Schwere der erhobenen Vorwürfe für verhältnismäßig hält.

Darüber hinaus entfällt der Schutz der Identität im Fall der vorsätzlichen Einmeldung unwahrer Hinweise.

Von einer von einem Hinweis betroffenen Person

Die Identität von einer von einem Hinweis betroffenen Person ist von den mit der Bearbeitung des Hinweises betrauten Personen zu schützen. Dies gilt auch für alle anderen Informationen, aus denen die Identität der vom Hinweis betroffenen Personen direkt oder indirekt abgeleitet werden kann.

Die Offenlegung der Identität einer von einem Hinweis betroffenen Person oder sonstiger Informationen, aus denen die Identität dieser Person direkt oder indirekt abgeleitet werden kann, ist dann zulässig, wenn eine Verwaltungsbehörde, ein Gericht oder die Staatsanwaltschaft dies im Rahmen des verwaltungsbehördlichen oder gerichtlichen Verfahrens oder eines

Ermittlungsverfahrens nach der StPO für unerlässlich und im Hinblick auf die Stichhaltigkeit und Schwere der erhobenen Vorwürfe für verhältnismäßig hält.

9. Datenschutzrechtliche Betroffenenrechte

Personen, deren personenbezogene Daten verarbeitet werden, haben das Recht auf Information, Auskunft, Berichtigung und Löschung. Sie können die Einschränkung der Verarbeitung der personenbezogenen Daten oder deren Übermittlung an eine andere verantwortliche Stelle bzw. die Ermöglichung des Rechts auf Datenübertragbarkeit gemäß den Vorgaben der DSGVO verlangen. Soweit personenbezogene Daten aufgrund eines berechtigten Interesses verarbeitet werden, kann Widerspruch gegen die Verarbeitung erhoben werden. Personen, die uns eine Einwilligungserklärung abgegeben haben, haben das Recht, ihre Einwilligungserklärung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Beschränkung der datenschutzrechtlichen Betroffenenrechte

Die datenschutzrechtlichen Betroffenenrechte (Recht auf Information, Recht auf Auskunft, Recht auf Berichtigung, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Recht auf Widerspruch, Recht auf Benachrichtigung einer Verletzung des Schutzes personenbezogener Daten) können eingeschränkt werden oder gänzlich entfallen, soweit und solange dies zum Schutz

- der Identität eines Hinweisgebers,
- natürlicher Personen, die Hinweisgeber bei der Hinweisgebung unterstützen,
- natürlicher Personen im Umkreis der Hinweisgeber, die, ohne die Hinweisgebung zu unterstützen, von nachteiligen Folgen der Hinweisgebung wie Vergeltungsmaßnahmen betroffen sein können,
- von Mitgliedern eines Verwaltungs-, Leitungs- oder Aufsichtsorgans des Rechtsträgers zu dem Hinweisgeber in beruflicher Verbindung stehen oder standen,

und zur Erreichung der Zwecke unseres Hinweisgebersystems, insbesondere um Versuche der Verhinderung, Unterlaufung oder Verschleppung von Hinweisen oder von Folgemaßnahmen aufgrund von Hinweisen zu unterbinden, erforderlich ist.

Allgemeine Information zur Ausübung datenschutzrechtlicher Betroffenenrechte

Ihre Rechte machen Sie durch eine formlose Mitteilung an den Datenschutzbeauftragten der steiermärkischen Raiffeisenbanken oder an die verantwortliche Stelle geltend. Sie erreichen uns unter:

Datenschutzbeauftragter:

Dipl. Ing. BSC Markus Hefler
Raiffeisen-Landesbank Steiermark AG
Radetzkystraße 15
8010 Graz
Oder:
datenschutz@rlbstmk.at

Verantwortliche Stelle Hinweissystem:

Raiffeisenverband Steiermark
Raiffeisen-Platz 11
8074 Raaba-Grambach
Oder:
datenschutz@rvstmk.at

Haben Sie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gegenüber uns geltend gemacht, sind wir verpflichtet, allen Empfängern, denen wir die Sie betreffenden personenbezogenen Daten offengelegt haben, diese Berichtigung oder Löschung der Daten oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als (rechtlich) unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Auf Verlangen informieren wir Sie über diese Empfänger.

Schließlich steht Ihnen unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. In Österreich können Beschwerden an die zuständige Datenschutzbehörde gerichtet werden (www.dsb.gv.at).

10. Anhang „weitere Rechtsgrundlagen“

Verletzungen der EU Marktmissbrauchsverordnung (MAR, Verordnung (EU) Nr. 596/2014), einschließlich der damit einhergehenden Bestimmungen des Börse- und Wertpapieraufsichtsgesetzes (§ 159 BörseG sowie § 98 WAG 2018),

Verletzungen des Finanzmarkt-Geldwäschegesetzes (FM-GwG), einer aufgrund des FM-GwG erlassenen Verordnung oder eines Bescheids oder Verletzungen der EU Geldwäscherichtlinie oder der Geldtransfer-Verordnung (EU) 2015/847 oder eines auf Basis dieser Verordnung erlassenen Bescheides,

Verletzungen der in § 70 Abs. 4 BWG aufgezählten Normen, und zwar:

- Bankwesengesetz (BWG)
- Sparkassengesetz
- Bausparkassengesetz (BSpG)
- Einführungsverordnung zum Hypothekenbank- und zum Pfandbriefgesetz
- Hypothekenbankgesetz (HypBG)
- Pfandbriefgesetz (PfandbriefG)
- fundierte Bankschuldverschreibungsgesetz (FBSchVG)
- Investmentfondsgesetz (InvFG)
- Depotgesetz (DepotG)
- E-Geldgesetz (EGG)
- Betriebliches Mitarbeiter- und Selbständigenvorsorgegesetz (BMSVG)
- Immobilien-Investmentfondsgesetz (ImmoInvFG)
- Finanzkonglomeratengesetz
- Bundesgesetz über die Sanierung und Abwicklung von Banken (BaSAG) Arbeitsanweisung Hinweisgebersystem/Whistle Blowing, Version 8.0, 04/2023 5/10
- Einlagensicherungs- und Anlegerentschädigungsgesetz (ESEAG)
- eine aufgrund der vorgenannten Bundesgesetze erlassene Verordnung oder ein Bescheid,
- Capital Requirements Regulation (CRR, Verordnung (EU) Nr. 575/2013) oder eines auf Basis der Verordnung erlassenen Bescheids
- der für die Bankenaufsicht relevanten technischen Standards im Sinne der Art. 10 bis 15 der Verordnung (EU) Nr. 1093/2010 und der Art. 10 bis 15 der Verordnung (EU) Nr. 1095/2010