Datenschutzinformation
Hinweisgebersystem

Das HinweisgeberInnenschutzgesetz sowie weitere finanzdienstleistungsspezifische Gesetze wie das FinanzmarktGeldwäschegesetz und das Börsegesetz 2018 verlangen die Administration und Organisation eines Hinweisgebersystems zur Meldung möglicher Missstände und Rechtsverstößen.

Der Schutz Ihrer persönlichen Daten ist uns dabei ein besonderes Anliegen. In dieser Datenschutzinformation informieren wir Sie über die wichtigsten Aspekte der Verarbeitung Ihrer personenbezogenen Daten im Rahmen einer Hinweisgebermeldung (Whistleblowing).

Bitte lesen Sie sich diese datenschutzrechtlichen Hinweise aufmerksam durch.

Hinweisgebersystem

Wir haben diverse Kanäle geschaffen, welche Meldungen von Missständen und Rechtsverstößen sowohl anonym als auch offen ermöglichen:

- E-Mail: compliance@vlv.at
- Telefon 05574/412-1295 (Compliance-Verantwortlicher)
- Postweg mit dem Adresszusatz „Compliance“ an den Compliance-Verantwortlichen
- Persönlicher Vorsprache bei der internen Stelle (Compliance-Verantwortlicher)
- Sämtliche Hinweise werden durch eine interne Melde-Stelle (Compliance-Verantwortlichen) angesiedelt, erfasst, verarbeitet und koordiniert.

Verantwortlicher für die Datenverarbeitung

Vorarlberger Landes-Versicherung V.a.G.
Bahnhofstraße 35
6900 Bregenz
Telefon: +43 5574-412-0
E-Mail (allgemein): vlv@vlv.at

Sollten Sie Fragen zur Verarbeitung Ihrer Daten haben, dann wenden Sie sich einfach an unseren Datenschutzbeauftragten unter der oben genannten Adresse mit dem Zusatz – Datenschutzbeauftragter – oder senden Sie eine E-Mail an: datenschutzbeauftragter@vlv.at

Zwecke der Datenverarbeitung / Rechtsgrundlage

Ein Hinweisgebersystem dient dazu, Hinweise auf Verstöße gegen rechtliche Bestimmungen und Compliance-Regelungen auf einem sicheren und vertraulichen Weg entgegenzunehmen, zu bearbeiten und zu verwalten. Die Verarbeitung von personenbezogenen Daten im Rahmen eines Hinweisgebersystems ist gestützt auf die im HinweisgeberInnenschutzgesetz, Finanzmarktgeldwäschegesetz und Börsegesetz 2018 geregelte rechtliche Verpflichtung von Versicherungsunternehmen. Ein Hinweisgebersystem dient der Aufdeckung und Prävention von Missständen und der Abwendung von Schaden für zB. Eigentümer, Mitarbeiter und Kunden.

Die Rechtsgrundlage dieser Verarbeitung von personenbezogenen Daten sind insbesondere Artikel 6 Abs. 1c DSGVO (rechtliche Verpflichtung) sowie für sensible Daten Ermächtigungen im HinweisgeberInnenschutzgesetz.

Arten der personenbezogenen Daten

Welche personenbezogenen Daten verarbeiten wir im Zusammenhang mit dem Abschluss eines Versicherungsvertrages (Art 13 DSGVO)?

Die Nutzung des Hinweisgebersystems erfolgt auf freiwilliger Basis. Wenn eine Meldung abgegeben wird, werden folgende personenbezogenen Daten und Informationen des Hinweisgebers erhoben:

- Namen, sofern die Hinweisgeber ihre Identität offenlegen,
- gegebenenfalls E-Mail-Adresse oder Postadresse,
- in welcher Beziehung die Hinweisgeber zu den Verantwortlichen stehen (Mitarbeiter, ehemaliger Mitarbeiter, Kunde, Lieferant, Dienstleister, Sonstiges),
- sonstige personenbezogene Daten zu der Person des Hinweisgebers, die in der Meldung genannt oder durch angehängte Dokumente offengelegt werden.

Welche personenbezogenen Daten verarbeiten wir von dritten Personen und woher stammen sie (Art 14 DSGVO)?

Wenn ein Hinweisgeber eine Meldung erstattet, dann können neben den Daten des Hinweisgebers auch personenbezogene Daten und Informationen von, in den gemeldeten Vorfall, involvierten Personen erhoben werden:

Version 1.1 - Stand: April 2020 / 4727

- Namen,
- sonstige personenbezogene Daten zu der Person, die in der Meldung genannt oder durch angehängte Dokumente offengelegt werden.

Empfänger / Kategorien von Empfängern

Sofern die Bearbeitung eines Hinweises ergeben hat, dass diesbezügliche Meldepflichten bestehen, erfolgt eine Mitteilung des Sachverhaltes an die zuständige(n) Strafverfolgungsbehörde(n).

Wir übermitteln grundsätzlich keine bezughabenden Daten an Empfänger außerhalb der EU. Bitte beachten Sie jedoch, dass die elektronische Kommunikation unter Verwendung handelsüblicher Mailprogramme (etwa MS Exchange) keinen absoluten Schutz vor Drittzugriffen bietet und dass bei dieser Form der Kommunikation auch Nicht-europäische Server eingeschaltet werden können.

Speicherdauer

Gemäß § 8 Abs. 1 HSchG sind die bezughabenden personenbezogene Daten zu löschen, sobald diese für die Besorgung der den Verantwortlichen obliegenden Aufgaben nicht mehr benötigt werden.

Eine Speicherung dieser personenbezogenen Daten erfolgt aber 30 Jahre ab ihrer letztmaligen Verarbeitung oder Übermittlung und jedenfalls für die Dauer jener Verfahren, zu welchen diese als Beweis benötigt werden. Protokolldaten sind gemäß § 8 Abs. 10 HSchG drei Jahre nach Entfall dieser 30-jährigen Aufbewahrungspflicht lang aufzubewahren.

Ihre Betroffenenrechte

Grundsätzlich haben Sie insbesondere das Recht auf Auskunft über die eine Person betreffenden, verarbeiteten Daten, sowie auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch (betrifft die Verarbeitung aufgrund öffentlichen Interesses oder berechtigten Interesses) und Datenübertragbarkeit unter jenen Voraussetzungen, welche in den bezughabenden, rechtlichen Bestimmungen (insbesondere den Art. 15 ff DSGVO) genannt sind.

Weiters haben Sie ein Beschwerderecht bei der für Sie zuständigen Aufsichtsbehörde. Kontaktdaten der österreichischen Datenschutzbehörde: Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at

Gemäß Art. 23 DSGVO iVm § 8 Abs. 7 HGSG können folgende Rechte von betroffenen Personen (jedenfalls bis zum Abschluss der Bearbeitung des bezughabenden Hinweises) zum Schutz einer hinweisgebenden Person bzw. zur Erreichung des in § 1 HSchG genannten Zwecks (Besorgung der Aufgaben nach dem HSchG) jedoch eingeschränkt sein: Recht auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruchsrecht sowie das Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten.

Ergänzende Informationen

Werden Ihre Hinweise vertraulich behandelt?

Unsere autorisierten Mitarbeiter in der internen Stelle prüfen den Sachverhalt und führen gegebenenfalls eine weitergehende fallbezogene Sachverhaltsaufklärung durch. Im Rahmen der Bearbeitung einer Meldung oder im Rahmen einer Sonderuntersuchung kann es notwendig sein, Hinweise weiteren Mitarbeitern in anderen Fachabteilungen weiterzugeben.

Jede Person, die Zugang zu den Daten erhält, ist zur Vertraulichkeit verpflichtet.

Kann die Identität des Hinweisgebers offengelegt werden?

Ohne ausdrückliche Zustimmung des Hinweisgebers wird die Identität des Hinweisgebers keiner anderen Person als gegenüber unseren autorisierten Mitarbeitern offengelegt. Abweichend davon erfolgt eine Offenlegung dann, wenn dies nach dem Unionsrecht oder dem nationalen Recht eine notwendige und verhältnismäßige Pflicht ist. Dies dient zB. der Untersuchung des Vorfalls durch Behörden und Gerichte.

Der Hinweisgeber wird vorab über die geplante Offenlegung informiert, es sei denn dies würde zB. die laufende Untersuchung gefährden.

Wie sicher werden Ihre personenbezogenen Daten übertragen und verarbeitet?

Wir verfügen über Verschlüsselungsoptionen im externen Datenverkehr, sofern Sie als Empfänger unserer Kommunikation, über die technischen Voraussetzungen zur Entschlüsselung verfügen. Bitte beachten Sie, dass die elektronische Kommunikation unter Verwendung handelsüblicher Mailprogramme (etwa MS Exchange) keinen absoluten Schutz vor Drittzugriffen bietet und dass bei dieser Form der Kommunikation auch Nicht-europäische Server eingeschaltet werden können. Für eine sichere Kommunikation können Sie unser Kontaktformular nutzen. Für die Übertragung der Daten, die Sie uns auf dieser Website zur Verfügung gestelltem Kontaktformular anvertrauen wollen, verwenden wir moderne Verschlüsselungstechniken (SSL-Verschlüsselung).

Auch gewährleisten wir, dass unsere unternehmensinterne IT gängige Sicherheitsstandards erfüllt. Unser Sicherheitsverständnis überbinden wir auch auf die von uns in Anspruch genommenen Dienstleister, welche wir zur Einhaltung gleichartiger oder ebenbürtiger Sicherheitsvorkehrungen verpflichten. Die Speicherung von Daten zu Ihrem Versicherungsverhältnis und die Speicherung von Ihren Gesundheitsdaten verbleibt stets in unserer internen IT. Sollten Sie Fragen zu unseren konkret Ihren Geschäftsfall betreffenden Datensicherheitsvorkehrungen haben, wenden Sie sich bitte mittels der allgemeinen E-Mail vlv@vlv.at oder über das Kontaktformular.