precis.

ITA - Whistleblowing Policy Precis Italia

Panoramica

Presso Precis, ci impegniamo per avere un ambiente di lavoro aperto e trasparente, dove non si verificano pratiche scorrette. È quindi importante per noi che ci siano informazioni chiare su come segnalare in modo confidenziale e sicuro. In caso di sospetto di pratiche scorrette in corso o precedenti, devono essere disponibili risorse per divulgarle. Facilitando la segnalazione, lavoriamo insieme per promuovere la fiducia dei dipendenti, dei clienti e del pubblico nei nostri confronti.

- **Chi può segnalare?**

È possibile segnalare e ricevere protezione ai sensi della legge sulla segnalazione di illeciti se si è dipendenti, volontari, tirocinanti, azionisti attivi, persone disponibili al lavoro sotto il nostro controllo e gestione o facenti parte dei nostri organi amministrativi, direttivi o di supervisione.
Anche appaltatori, subappaltatori e fornitori che hanno scoperto pratiche scorrette all'interno di Precis possono segnalare. Il fatto che tu abbia terminato o non iniziato il tuo rapporto di lavoro con noi non è un ostacolo per segnalare pratiche scorrette o ricevere protezione per la segnalazione di pratiche scorrette all'esterno.
Inoltre, consentiamo anche a persone al di fuori delle categorie sopra indicate di utilizzare il nostro canale di segnalazione interno. Tratteremo tutte le segnalazioni allo stesso modo, anche se tu, come esterno, non sei coperto dalla protezione della legge sulla segnalazione di illeciti.

- **Cosa posso segnalare?**

In caso di sospetto di possibili comportamenti scorretti, violazioni di leggi e/o regolamenti, ti invitiamo a segnalarlo come caso di segnalazione di illeciti. Al momento della segnalazione, è importante che tu abbia avuto motivi ragionevoli per credere che le informazioni sul comportamento scorretto segnalato fossero vere. La valutazione se ci fossero motivi ragionevoli, circostanze e informazioni disponibili al momento della segnalazione dovrebbe essere la base per stabilire se potevi presumere che il comportamento scorretto fosse vero. Inoltre, è importante che il comportamento possa effettivamente essere considerato una violazione segnalabile e quindi garantirti protezione contro le ritorsioni.

- **Illeciti di interesse pubblico**

Puoi segnalare informazioni su comportamenti scorretti emersi in un contesto lavorativo per cui c'è un interesse pubblico nel farli emergere. In caso di altri tipi di lamentele personali che non hanno un interesse pubblico nel venire alla luce, come dispute o lamentele riguardanti il luogo di

lavoro o l'ambiente lavorativo, ti incoraggiamo a contattare il tuo responsabile diretto e/o il reparto delle risorse umane. Questo per garantire che tali questioni siano gestite nel modo migliore possibile.

Precis S.r.l.
Sede Legale: Via Aurelia Sud 23/E, Pietrasanta (LU) 55045
Registro Imprese di Lucca: LU - 225491
Codice Fiscale e Partita Iva: 02435610460
Pec: boosterboxsrl@pec.it
https://www.precis.com/it

Esempi di pratiche gravi che dovrebbero essere segnalate:

- Contabilità deliberatamente scorretta, controllo interno della contabilità o altri reati finanziari.
- Casi di furto, corruzione, vandalismo, frode, appropriazione indebita o hacking.
- Crimini ambientali gravi o gravi carenze nella sicurezza sul lavoro.
- Se qualcuno è esposto a forme molto gravi di discriminazione o molestie.
- Altri comportamenti gravi che influenzano la vita o la salute delle persone.

All'interno della nostra azienda, abbiamo scelto di considerare anche tutti i comportamenti non etici o illegali come irregolarità meritevoli di segnalazione. Trattiamo quindi tutte le segnalazioni ricevute allo stesso modo, basandoci sull'intenzione della legge e fornendo protezione contro le ritorsioni per tutti.
Se la segnalazione non soddisfa i criteri della legge sulla segnalazione di illeciti, la legge stessa non può fornire protezione, e quindi forniremo comunque la stessa riservatezza e protezione contro le ritorsioni di una segnalazione secondo la legge sulla segnalazione di illeciti, a condizione che la segnalazione sia vera e/o fatta in buona fede.
Di seguito sono riportati esempi di comportamenti non etici o illegali che potrebbero essere segnalati:

- Azioni e omissioni contrarie alla nostra cultura, visione e valori.
- Comportamenti contrari alla buona prassi e agli standard del mercato del lavoro.
- Atti pericolosi che potrebbero causare danni fisici a persone o proprietà.
- Discriminazione di qualsiasi tipo.
- Sfruttamento di posizione e/o abuso di potere.
- Comportamenti contrari al diritto dell'UE

Inoltre, c'è la possibilità di segnalare informazioni su comportamenti scorretti emersi in un contesto lavorativo che è contrario alle leggi o ai regolamenti dell'UE. Se sospetti che ciò accada, leggi la portata della Direttiva sulla segnalazione di illeciti all'articolo 2 e all'Allegato Parte 1 per le leggi applicabili.

- **Come posso segnalare?**
  - Canali di segnalazione
    - interno (nell'ambito del contesto lavorativo);
    - esterno (ANAC);
  - divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
  - denuncia all'Autorità giudiziaria o contabile.
  - Scelta del canale di segnalazione

Precis S.r.l.
Sede Legale: Via Aurelia Sud 23/E, Pietrasanta (LU) 55045
Registro Imprese di Lucca: LU - 225491
Codice Fiscale e Partita Iva: 02435610460
Pec: boosterboxsrl@pec.it
https://www.precis.com/it

I segnalanti possono utilizzare il canale esterno (ANAC) quando:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto richiesto dalla legge;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

I segnalanti possono effettuare direttamente una divulgazione pubblica quando:

- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

- **Segnalazione scritta**

Per la segnalazione scritta, utilizziamo Visslan, che è il nostro canale digitale per le segnalazioni. È sempre disponibile su https://precisdigital.visslan-report.se/#/. Sul sito web, scegli "segnala" per poter descrivere il comportamento sospetto. Descrivi quanto accaduto il più dettagliatamente possibile, in modo che possiamo garantire l'applicazione di misure adeguate. È anche possibile allegare prove aggiuntive, come documenti scritti, immagini o file audio, anche se questo non è obbligatorio.

- **Dati personali sensibili**

Non includere dati personali sensibili sulle persone menzionate nella tua segnalazione a meno che non sia necessario per descrivere il tuo caso. I dati personali sensibili includono

informazioni su origine etnica, opinione politica, convinzioni religiose o filosofiche, iscrizione sindacale, salute, vita sessuale o orientamento sessuale di una persona, dati genetici, dati biometrici utilizzati per identificare un individuo.

- **Anonimato**

Puoi rimanere anonimo per tutto il processo senza compromettere la tua protezione legale, ma hai anche l'opportunità di rivelare la tua identità sotto rigorosa riservatezza. L'anonimato può in alcuni casi complicare le possibilità di follow-up della segnalazione e le misure che possiamo adottare, ma in tal caso possiamo chiederti successivamente di rivelare la tua identità, sempre in rigorosa riservatezza ai Responsabili del Caso.

- **Follow-up e accesso**

Dopo aver segnalato, riceverai un codice di sedici cifre, con il quale potrai accedere a Visslan su https://precisdigital.visslan-report.se/#/. È molto importante che tu salvi il codice, altrimenti non potrai accedere nuovamente alla tua segnalazione.
Se perdi il codice, puoi inviare una nuova segnalazione facendo riferimento alla segnalazione precedente.
Entro sette giorni, riceverai la conferma che il/la Responsabile del Caso ha ricevuto la tua segnalazione. Il/la Responsabile del Caso è la parte indipendente e autonoma che riceve le segnalazioni nel canale di segnalazione, la cui informazione di contatto è allegata alla Sezione
6.1 Informazioni di contatto per il/la Responsabile del Caso. In caso di domande o preoccupazioni, tu e il/la Responsabile del Caso potete comunicare tramite la funzione di chat integrata e anonima della piattaforma. Riceverai un feedback entro tre mesi su qualsiasi misura pianificata o attuata a seguito della segnalazione.
È importante che tu, con il tuo codice di sedici cifre, acceda regolarmente per rispondere a eventuali domande di follow-up del/dei Responsabile/i del Caso. In alcuni casi, la segnalazione non può procedere senza risposte a tali domande di follow-up da parte tua come persona che segnala.

- **Segnalazione verbale**

Inoltre, è possibile effettuare una segnalazione verbale caricando un file audio come allegato durante la creazione di una segnalazione su https://precisdigital.visslan-report.se/#/. Puoi farlo selezionando di avere prove per la segnalazione e caricando un file audio Ii. Nel file audio, descrivi gli stessi fatti e dettagli che avresti fatto in un caso scritto.
Inoltre, è possibile richiedere un incontro fisico con il/la Responsabile del Caso tramite Visslan. Questo può essere fatto più facilmente richiedendolo in una segnalazione esistente o creandone una nuova che richieda un incontro fisico.

- **Segnalazione esterna**

Ti invitiamo a segnalare sempre prima le pratiche scorrette internamente, ma in caso di difficoltà o se considerato inappropriato, è possibile effettuare una segnalazione esterna (o dopo una segnalazione interna senza risultati). In tal caso, ti indirizziamo a contattare le autorità competenti o, se del caso, le istituzioni, gli organi o le agenzie dell'UE.

- **Quali sono i miei diritti?**

    - **Diritto alla riservatezza**

Durante la gestione della segnalazione, garantiremo che la tua identità come persona che segnala sia trattata in modo riservato e che l'accesso al caso sia impedito al personale non autorizzato, cioè al/ai Responsabile/i del Caso. Non divulgaremo la tua identità senza il tuo consenso se la legge applicabile non ci obbliga a farlo e ci assicureremo che tu non sia soggetto a ritorsioni.

    - **Protezione contro rappresaglie o ritorsioni**

In caso di segnalazione, c'è protezione contro conseguenze negative per aver segnalato comportamenti scorretti sotto forma di divieto di ritorsioni e ritorsioni. La protezione contro ciò si applica anche, nei casi pertinenti, alle persone sul luogo di lavoro che assistono la persona che segnala, ai tuoi colleghi e parenti sul luogo di lavoro e alle persone giuridiche di tua proprietà, per cui lavori o che sono comunque collegate a te.
Ciò significa che non sono permesse minacce di ritorsioni e tentativi di ritorsioni. Esempi di ciò sono se dovessi essere licenziato, costretto a cambiare compiti, subire misure disciplinari, minacce, discriminazioni, essere inserito in una lista nera nella tua industria, o simili a causa della segnalazione.
Anche se dovessi essere identificato e subire ritorsioni, saresti comunque coperto dalla protezione fintanto che avessi motivi ragionevoli per credere che il comportamento segnalato fosse vero e rientrante nel campo di applicazione della legge sulla segnalazione di illeciti. Nota, tuttavia, che la protezione non è ottenuta se è un reato acquisire o avere accesso alle informazioni segnalate.
La protezione contro le ritorsioni si applica anche nei procedimenti legali, compresa diffamazione, violazione del diritto d'autore, violazione della riservatezza, violazione delle norme sulla protezione dei dati, divulgazione di segreti commerciali o azioni per danni basate sul diritto privato, diritto pubblico o diritto del lavoro collettivo, e non sarai ritenuto responsabile in alcun modo a causa delle segnalazioni o delle divulgazioni fornite a condizione che tu avessi motivi ragionevoli per credere che fosse necessario segnalare o pubblicare tali informazioni per denunciare un comportamento scorretto.

    - **Pubblicazione delle informazioni**

La protezione si applica anche alla pubblicazione delle informazioni. Si presume quindi che tu abbia segnalato internamente all'interno dell'azienda e esternamente a un'autorità governativa, o direttamente esternamente, e che nessuna azione appropriata sia stata intrapresa entro tre mesi (in casi giustificati sei mesi). La protezione è ottenuta anche quando hai avuto motivi ragionevoli per credere che possa esserci un evidente pericolo per l'interesse pubblico se non viene reso pubblico, ad esempio in caso di emergenza. Lo stesso si applica quando c'è il rischio di ritorsioni nel caso di segnalazioni esterne o è improbabile che la cattiva condotta venga corretta in modo efficace, ad esempio nel caso in cui esista il rischio che le prove possano essere nascoste o distrutte.

- **Diritto di consultare la documentazione durante gli incontri con i Case Manager**

Se hai richiesto un incontro con i Case Manager, essi, con il tuo consenso, garantiranno che la documentazione completa e corretta dell'incontro sia conservata in modo duraturo e accessibile. Ciò può essere fatto, ad esempio, registrando la conversazione o prendendo appunti. Successivamente, avrai l'opportunità di verificare, correggere e approvare il protocollo firmandolo.
Raccomandiamo che questa documentazione sia conservata sulla piattaforma di Visslan, creando un caso in cui le informazioni possano essere raccolte in modo sicuro, con la possibilità di comunicare in modo sicuro.

- **GDPR e gestione dei dati personali**

Facciamo sempre il massimo per proteggerti e proteggere le tue informazioni personali. Garantiamo quindi che il nostro trattamento di queste informazioni sia sempre in conformità con il Regolamento Generale sulla Protezione dei Dati ("GDPR").
Inoltre, tutti i dati personali non rilevanti per il caso saranno cancellati, e il caso verrà conservato solo per il tempo necessario e proporzionato. Il periodo massimo di elaborazione di un caso è di due anni dalla sua conclusione. Per ulteriori informazioni sulla nostra gestione dei dati personali, consulta l'informativa sulla privacy di Precis.

- **Contatti aggiuntivi**

Se hai ulteriori domande su come gestiamo i casi di segnalazione, sei sempre il benvenuto a contattare i Case Manager.
Per domande tecniche sulla piattaforma Visslan, sentiti libero di creare un caso su https://precisdigital.visslan-report.se. Se ciò non fosse possibile, contatta Visslan. Le informazioni di contatto per entrambi si trovano di seguito.

- **Informazioni di contatto per i Case Manager**

Persone di contatto interne Nome: Mikaela Diamantidis

Posizione: Generalista HR

Email: diamantidis@precisdigital.com Numero di telefono: +46 765 369 316
Nome: Jasmine Daniel Harris Posizione: Consulente Legale Email: jasmine@precisdigital.com
Numero di telefono: +44 7849 702833

- **Informazioni di contatto per Visslan (The Whistle Compliance Solutions AB)**

Email: clientsupport@visslan.com Numero: +46 10-750 08 10
Numero diretto (Daniel Vaknine): +46 73 540 10 19

========

Definizioni

GDPR: Regolamento Generale sulla Protezione dei Dati, che è una normativa europea che disciplina il trattamento dei dati personali e la libera circolazione di tali dati all'interno dell'Unione Europea.
Direttiva Whistleblower: Direttiva UE 2019/1936 sulla protezione delle persone che segnalano irregolarità nel diritto dell'Unione.
Legge Whistleblower: Implementazione nazionale della Direttiva Whistleblower negli Stati membri dell'UE.
Visslan: Il servizio Visslan di The Whistle Compliance Solutions AB, che consente la segnalazione digitale di cattiva condotta: https://visslan.com/
Cattiva condotta: Azioni o omissioni emerse in un contesto legato al lavoro che presentano un interesse pubblico.
Segnalazione: Presentazione scritta o verbale di informazioni sulla cattiva condotta.
Segnalazione interna: Presentazione scritta o verbale di informazioni sulla cattiva condotta all'interno di un'azienda nel settore privato.
Segnalazione esterna: Presentazione scritta o verbale di informazioni sulla cattiva condotta alle autorità competenti.
Pubblicazione o rendere pubblico: Rendere disponibili al pubblico informazioni sulla cattiva condotta.
Segnalante: Una persona che segnala o pubblica informazioni sulla cattiva condotta acquisite nel contesto delle sue attività legate al lavoro.
Ritorsione: Qualsiasi atto o omissione diretto o indiretto che si verifica in un contesto lavorativo e che è causato dalla segnalazione interna o esterna o dalla pubblicazione, e che comporta o può comportare un danno ingiustificato alla persona che segnala.
Seguito: Qualsiasi azione intrapresa dai Case Manager per valutare l'accuratezza delle accuse fatte nella segnalazione e, se del caso, per affrontare l'infrazione segnalata, anche attraverso misure come indagini interne, indagini, azioni legali per recuperare fondi e per chiudere la procedura.
Feedback: Fornire ai segnalatori ("whistleblowers") informazioni sulle azioni pianificate o intraprese come seguito e sulle ragioni di tale seguito.

Precis S.r.l.
Sede Legale: Via Aurelia Sud 23/E, Pietrasanta (LU) 55045
Registro Imprese di Lucca: LU - 225491
Codice Fiscale e Partita Iva: 02435610460
Pec: boosterboxsrl@pec.it
https://www.precis.com/it

precis.

ENG - Whistleblowing Policy Precis Italy

Overview

At Precis, we are committed to maintaining an open and transparent work environment where no misconduct occurs. Therefore, it is important to us that there is clear information on how to report confidentially and safely. In case of suspected ongoing or previous misconduct, resources must be available to disclose it. By facilitating reporting, we work together to promote the trust of our employees, customers, and the public in us.

Who Can Report?

You can report and receive protection under the whistleblowing law if you are an employee, volunteer, trainee, active shareholder, persons available to work under our control and management, or part of our administrative, executive, or supervisory bodies.

Contractors, subcontractors, and suppliers who have discovered misconduct within Precis may also report. The fact that you have terminated or not begun your employment relationship with us is not an obstacle to reporting misconduct or receiving protection for reporting misconduct externally.

Furthermore, we also allow persons outside the categories mentioned above to use our internal reporting channel. We will treat all reports in the same manner, even if you, as an external party, are not covered by the protection of the whistleblowing law.

What Can I Report?

In case of suspected possible misconduct, violations of laws and/or regulations, we invite you to report it as a case of whistleblowing. At the time of reporting, it is important that you had reasonable grounds to believe that the information about the reported misconduct was true. The assessment of whether there were reasonable grounds, circumstances, and information available at the time of reporting should be the basis for establishing whether you could assume the misconduct was true. Furthermore, it is important that the conduct can actually be considered a reportable violation and thus guarantee you protection against retaliation.

Matters of Public Interest

You can report information about misconduct that emerged in a work context for which there is public interest in its disclosure. In case of other types of personal complaints that do not have public interest in coming to light, such as disputes or complaints regarding the workplace or work environment, we encourage you to contact your direct manager and/or the human resources department. This is to ensure that such matters are handled in the best possible way.

Examples of Serious Misconduct That Should Be Reported:

- Deliberately incorrect accounting, internal accounting controls, or other financial crimes.
- Cases of theft, corruption, vandalism, fraud, embezzlement, or hacking.
- Serious environmental crimes or serious deficiencies in workplace safety.
- If someone is exposed to very serious forms of discrimination or harassment.
- Other serious behaviors that affect the lives or health of people.

Within our company, we have chosen to consider all unethical or illegal behaviors as irregularities worthy of reporting. We therefore treat all reports received in the same way, based on the intention of the law and providing protection against retaliation for all.

If the report does not meet the criteria of the whistleblowing law, the law itself cannot provide protection, and we will therefore still provide the same confidentiality and protection against retaliation as a report under the whistleblowing law, provided that the report is true and/or made in good faith.
The following are examples of unethical or illegal behaviors that could be reported:

- Actions and omissions contrary to our culture, vision, and values.
- Behaviors contrary to good practice and standards in the labor market.
- Dangerous acts that could cause physical harm to persons or property.
- Discrimination of any kind.
- Abuse of position and/or abuse of power.
- Behaviors contrary to EU law

Additionally, there is the possibility of reporting information about misconduct that emerged in a work context that is contrary to EU laws or regulations. If you suspect this is happening, read the scope of the Whistleblower Directive in Article 2 and Annex Part 1 for applicable laws.

How Can I Report?

Reporting Channels

- Internal (within the work context);
- External (ANAC);
- Public disclosure (via press, electronic means, or means of dissemination capable of reaching a large number of people);
- Report to the Judicial or Accounting Authority.

Choice of Reporting Channel

Reporters can use the external channel (ANAC) when:

- Activation of the internal reporting channel is not required within the work context, or this, even if mandatory, is not active, or, even if activated, does not comply with what is required by law;
- The reporting person has already made an internal report and the same has not been followed up;
- The reporting person has reasonable grounds to believe that, if they made an internal report, it would not be effectively followed up or that the same report could determine a risk of retaliation;
- The reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest;

Reporters can directly make a public disclosure when:

- The reporting person has previously made an internal and external report or has directly made an external report and no response has been given within the established timeframes regarding the measures provided or taken to follow up on the reports;
- The reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest;
- The reporting person has reasonable grounds to believe that external reporting may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances

of the case, such as those in which evidence could be concealed or destroyed, or in which there is reasonable fear that the person who received the report may be colluding with the author of the violation or involved in the violation itself.

Written Report

For written reporting, we use Visslan, which is our digital channel for reports. It is always available at https://precisdigital.visslan-report.se/#/. On the website, choose "report" to be able to describe the suspected behavior. Describe what happened in as much detail as possible, so we can ensure the application of appropriate measures. It is also possible to attach additional evidence, such as written documents, images, or audio files, although this is not mandatory.

Sensitive Personal Data

Do not include sensitive personal data about the persons mentioned in your report unless necessary to describe your case. Sensitive personal data includes information on ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation of a person, genetic data, biometric data used to identify an individual.

Anonymity

You can remain anonymous throughout the process without compromising your legal protection, but you also have the opportunity to disclose your identity under strict confidentiality. Anonymity may in some cases complicate the possibilities of follow-up to the report and the measures we can take, but in that case we may ask you later to reveal your identity, always in strict confidentiality to the Case Managers.

Follow-up and Access

After reporting, you will receive a sixteen-digit code, with which you can access Visslan at https://precisdigital.visslan-report.se/#/. It is very important that you save the code, otherwise you will not be able to access your report again.
If you lose the code, you can submit a new report by referring to the previous report.
Within seven days, you will receive confirmation that the Case Manager has received your report. The Case Manager is the independent and autonomous party that receives reports in the reporting channel, whose contact information is attached to Section 6.1 Contact Information for the Case Manager. If you have questions or concerns, you and the Case Manager can communicate via the platform's integrated anonymous chat function. You will receive feedback within three months on any measures planned or taken as a result of your report.
It is important that you, with your sixteen-digit code, regularly access to respond to any follow-up questions from the Case Manager(s). In some cases, the report cannot proceed without responses to such follow-up questions from you as the reporting person.

Oral Report

Furthermore, it is possible to make an oral report by uploading an audio file as an attachment when creating a report at https://precisdigital.visslan-report.se/#/. You can do this by selecting that you have evidence for the report and uploading an audio file there. In the audio file, describe the same facts and details that you would have done in a written case.

Furthermore, it is possible to request a physical meeting with the Case Manager via Visslan. This can be done more easily by requesting it in an existing report or by creating a new one requesting a physical meeting.

External Report

We invite you to always report misconduct internally first, but in case of difficulties or if considered inappropriate, it is possible to make an external report (or after an internal report without results). In that case, we direct you to contact the competent authorities or, where applicable, EU institutions, bodies, or agencies.

What Are My Rights?

Right to Confidentiality

During the handling of your report, we will ensure that your identity as a reporting person is treated confidentially and that access to the case is prevented for unauthorized personnel, i.e., the Case Manager(s). We will not disclose your identity without your consent if applicable law does not require us to do so, and we will ensure that you are not subject to retaliation.

Protection Against Reprisals or Retaliation

In case of reporting, there is protection against negative consequences for reporting misconduct in the form of a prohibition on retaliation and reprisals. Protection against this also applies, where relevant, to persons in the workplace who assist the reporting person, your colleagues and relatives in the workplace, and legal entities you own, work for, or are otherwise connected to you.

This means that threats of retaliation and attempts at retaliation are not permitted. Examples of this are if you were to be fired, forced to change duties, subject to disciplinary measures, threats, discrimination, be blacklisted in your industry, or similar due to reporting.

Even if you were to be identified and suffer retaliation, you would still be covered by protection as long as you had reasonable grounds to believe that the reported behavior was true and fell within the scope of the whistleblowing law. Note, however, that protection is not obtained if it is a crime to acquire or have access to the reported information.

Protection against retaliation also applies in legal proceedings, including defamation, copyright infringement, breach of confidentiality, violation of data protection regulations, disclosure of trade secrets, or claims for damages based on private law, public law, or collective labor law, and you will not be held responsible in any way because of the reports or disclosures provided as long as you had reasonable grounds to believe it was necessary to report or publish such information to denounce misconduct.

Publication of Information

Protection also applies to the publication of information. It is therefore assumed that you have reported internally within the company and externally to a government authority, or directly externally, and that no appropriate action has been taken within three months (in justified cases six months). Protection is also obtained when you have had reasonable grounds to believe that there may be an evident danger to the public interest if it is not made public, for example in case of emergency. The same applies when there is a risk of retaliation in the case of external reports or it is unlikely that the

misconduct will be corrected effectively, for example in the case where there is a risk that evidence could be hidden or destroyed.

Right to Consult Documentation During Meetings with Case Managers

If you have requested a meeting with Case Managers, they will, with your consent, ensure that complete and accurate documentation of the meeting is retained in a durable and accessible manner. This can be done, for example, by recording the conversation or taking notes. Subsequently, you will have the opportunity to verify, correct, and approve the protocol by signing it.
We recommend that this documentation be retained on the Visslan platform, by creating a case in which information can be collected securely, with the possibility of communicating securely.

GDPR and Personal Data Management

We always do our utmost to protect you and your personal information. We therefore ensure that our processing of this information is always in compliance with the General Data Protection Regulation ("GDPR").
Furthermore, all personal data not relevant to the case will be deleted, and the case will be retained only for as long as necessary and proportionate. The maximum period for processing a case is two years from its conclusion. For further information on our handling of personal data, please consult Precis's privacy notice.

Additional Contacts

If you have further questions about how we handle reporting cases, you are always welcome to contact the Case Managers.
For technical questions about the Visslan platform, feel free to create a case at https://precisdigital.visslan-report.se. If this is not possible, contact Visslan. Contact information for both can be found below.

Contact Information for Case Managers

Internal Contacts

Name: Mikaela Diamantidis **Position:** HR Generalist **Email:** diamantidis@precisdigital.com **Phone:** +46 765 369 316
Name: Jasmine Daniel Harris **Position:** Legal Consultant **Email:** jasmine@precisdigital.com **Phone:** +44 7849 702833

Contact Information for Visslan (The Whistle Compliance Solutions AB)

Email: clientsupport@visslan.com **Phone:** +46 10-750 08 10 **Direct Line (Daniel Vaknine):** +46 73 540 10 19

Definitions

GDPR: General Data Protection Regulation, which is a European regulation that governs the processing of personal data and the free movement of such data within the European Union.

Whistleblower Directive: EU Directive 2019/1936 on the protection of persons reporting irregularities in EU law.

Whistleblower Law: National implementation of the Whistleblower Directive in EU Member States.

Visslan: The Visslan service of The Whistle Compliance Solutions AB, which enables digital reporting of misconduct: https://visslan.com/

Misconduct: Actions or omissions that emerged in a work-related context that present public interest.

Report: Written or oral presentation of information about misconduct.

Internal Report: Written or oral presentation of information about misconduct within a company in the private sector.

External Report: Written or oral presentation of information about misconduct to the competent authorities.

Publication or Making Public: Making information about misconduct available to the public.

Reporter: A person who reports or publishes information about misconduct acquired in the context of his or her work-related activities.

Retaliation: Any direct or indirect act or omission that occurs in a work context and is caused by internal or external reporting or publication, and that causes or may cause unjustified harm to the reporting person.

Follow-up: Any action taken by the Case Managers to evaluate the accuracy of the allegations made in the report and, where appropriate, to address the reported violation, including through measures such as internal investigations, investigations, legal action to recover funds, and to close the procedure.

Feedback: Providing whistleblowers with information on the actions planned or taken as follow-up and the reasons for such follow-up.

Precis S.r.l.
Sede Legale: Via Aurelia Sud 23/E, Pietrasanta (LU) 55045
Registro Imprese di Lucca: LU - 225491
Codice Fiscale e Partita Iva: 02435610460
Pec: boosterboxsrl@pec.it
https://www.precis.com/it