WHISTLEBLOWING POLICY OF ASPÖCK GROUP

aspoeck.com

WHISTLEBLOWING

WHISTLEBLOWING MISSION STATEMENT

We are committed to creating a culture of openness, transparency, integrity and accountability, where our workforce and other stakeholders, such as customers and suppliers, feel comfortable reporting breaches without fear of retaliation.

We encourage individuals to use our internal reporting channel to inform us of any breaches. This allows us to identify and address them at the earliest opportunity, take appropriate measures, prevent further misconduct and limit potential financial, reputational, environmental, human and other detrimental impacts.

We are committed to ensuring that the reported breaches are processed diligently and confidentially, applying the principles of trust, impartiality and protection, providing appropriate feedback throughout the entire process. In this sense, we undertake to continually improve our whistleblowing management system.

This whistleblowing policy is not a substitute for managers taking responsibility for their workplace and it does not prevent an individual reporting to the relevant authorities.

WHO DOES THIS POLICY APPLY TO?

This policy applies to whistleblowers. Whistleblowers are reporting persons who acquired information on breaches in a workrelated context. This includes, but is not limited to, our current and previous employees, self-employed persons, shareholders and persons belonging to tWhihe management or supervisory body of our company, including their non-executive members, as well as volunteers, paid or unpaid trainees, clients, customers and any persons working under the supervision and direction of our joint venture partners, contractors, subcontractors and suppliers. This policy shall also apply to whistleblowers whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations. Protection under this policy shall also be provided to persons assisting whistleblowers in the reporting process (facilitators), third persons who are connected with the whistleblower (colleagues or relatives) and who could suffer retaliation in a work-related context, and legal entities that the whistleblower owns, works for or is otherwise connected with in a work-related context. We hereby comply with legal requirements set by Directive (EU) 2019/1937 and implemented in national law • Portugal: Law n° 93/2021 from December 20th, 2021: General Regime for the Protection of Whistleblowers of Infractions.

WHAT TO REPORT?

The internal reporting channel is intended for reports, where a whistleblower has at least reasonable suspicion about actual or potential breaches, which occurred, are currently ongoing, or are very likely to occur, and about attempts to conceal such breaches. A breach is any act or omission that is unlawful and relates to Aspöck, or defeats the object or the purpose of legislation, our policies and/or internal regulations. A breach can include, but is not limited to, the following:

- bribery or corruption • fraud, money laundering, theft or improper use of company property or funds,
- undeclared or mismanaged conflicts of interest,
- anti-competitive behaviour,
- insider trading or market abuse,
- breach of sanctions,
- financial irregularities,
- data privacy violations,
- gross negligence, bullying,
- unlawful discrimination
- workplace or sexual harassment,
- gross waste or mismanagement,
- unsafe work practices and other significant safety or health concerns,
- modern slavery and human rights breaches,
- significant harm to the environment,
- retaliation against a whistleblower or other protected person under this policy and,
- any other conduct which is unethical, in breach of Aspöck policies or procedures, or illegal or unlawful.

The internal reporting channel is not intended for submitting complaints, warranty claims etc. Such reports will not be processed under this policy. For addressing latter issues, please refer to your known contact within the Organization.

HOW TO REPORT?

The authorised staff (details see below) is available to provide support or advice on Aspöck's whistleblowing process.

Reporting Channels

Reports can be submitted by using Aspöck's online whistleblowing solution "Trusty" available under

- Aspöck Austria and Aspöck Group: www.aspoeck.at/whistleblowing
- Aspöck Portugal: www.aspoeck.pt/whistleblowing
- Aspöck Poland: www.aspoeck.net.pl/whistleblowing

Alternatively, reports can be made via the intranet

- https://intranet.aspoeck.com/whistleblowing

Moreover, subjects can be addressed directly to

- whistleblowing@aspoeck.at (for Aspöck Austria and Group issues)
- whistleblowing@aspoeck.pt (for issues regarding Aspöck Portugal
- whistleblowing@aspoeck.net.pl (for issues regarding Aspöck Portugal)

in case the whistleblower is not requesting anonymity or has different questions with regard to whistleblowing.

When submitting reports through the above listed channels, whistleblowers are encouraged to provide contact details to which they wish to receive report receipt acknowledgments and feedback on their reports from Aspöck.

Content and Whistleblower's Identity

A report should include as much details as possible on who, what, where, when, how and why in relation to the reported breach, as well as any evidence in support thereof. Any other information as to how Aspöck might best go about processing the reported breach are also welcome.

Whistleblowers may submit reports anonymously or may choose to disclose their identity. The Whistleblowing software allows for a two-way anonymous communication even if a whistleblower chooses to report a breach without disclosing his or her identity. Whistleblowers are encouraged to identify themselves. This allows for a more productive and efficient processing of their reports and their protection against retaliation.

The whistleblowers' identities, as well as any other information from which their identities may be directly or indirectly deduced, shall not be disclosed to anyone beyond the authorised staff members competent to receive and follow up on reports, without whistleblowers' explicit consents. Notwithstanding the preceding provision, Aspöck shall disclose a whistleblower's identity when required to do so by law, whereby it shall inform the whistleblower thereof before such disclosure, unless such information would jeopardise the related investigations or judicial proceedings.

Any unauthorised attempts to identify a whistleblower or a concerned person are not allowed and shall be disciplinarily sanctioned.

BY WHOM AND HOW ARE REPORTS PROCESSED?

Authorised Staff

Aspöck's internal reporting channel is operated by the respective compliance department. who is authorised to receive and follow up on reports (herein referred to as the authorised staff). The authorised staff has direct, unrestricted and confidential access to Aspöck's governing body and top management to which it directly reports on the performance of the whistleblowing management system. The authorised staff has direct, unrestricted access to adequate resources as necessary to ensure the impartiality, integrity and transparency of the whistleblowing management system and its processes.

Processing of the reports

Processing of a report is conducted in the following steps, depending on the content of the report and its nature:

- received – the report has been received by Aspöck;
- initial triage – the content of the report is being assessed for the purposes of categorization (Whistleblowing case, Non Whistleblowing case but miscellaneous compliance, Non-Whistleblowing case), taking preliminary measures, prioritization and assignment for further handling;
- processed – the report is being handled, accuracy of the allegation is being assessed, internal enquiry or action for recovery of funds is being conducted;
- in investigation – the allegation is being investigated;
- closed – the processing of the report has been completed; either no action is considered necessary in response to a report, fact-finding determines no further investigation is warranted, the report is referred to another process to be dealt with, or the investigation has been completed (whether or not breach is confirmed).

Aspöck aims to process the reports in a timely manner. Circumstances such as the complexity of the reported breach, competing priorities and other compelling reasons may require an extended period for the completion of the processing of the report. Aspöck processes the reports confidentially, impartially, and without bias or prejudice against the whistleblower or any other person involved in, or any witness to, the reported breach.

The persons concerned, i.e. the persons referred to in the reports, shall enjoy the presumption of innocence. They may be notified of the respective reports at an appropriate time. Any investigation shall be conducted in a manner that preserves confidentiality to the extent possible and appropriate to ensure that the persons concerned are not exposed to reputational harm (information is shared on a strictly need-to-know basis).

Communication with Whistleblowers

After submitting a report the whistleblower shall receive a receipt acknowledgment forthwith and no later than within seven days of that receipt. The receipt acknowledgment is sent to the email address which is provided by the whistleblower during the online report submission process. The confirmation of the receipt of the report is also provided in the whistleblower's inbox which is accessible online under the reporting channels using the log-in credentials which are provided to the whistleblower upon the completion of the report submission process. The latter are provided also to anonymous whistleblowers. The authorised staff maintains communication with the whistleblower and, where necessary, asks for further information or evidence from and provide feedback to the whistleblower. The said communication is conducted through the whistleblower's inbox, or through other communication channels agreed with the whistleblower. The feedback to the whistleblower is provided no later than 3 months from submitting the report. The feedback includes information on the action envisaged or taken as follow-up and on the grounds for such follow-up. The feedback can be limited to avoid compromising any investigation or other legal proceedings, as well as due to legal restrictions on what can be communicated about the follow-up and findings. In such a case and where possible, the whistleblower shall be notified of the reasons of the limited feedback communication. Aspöck may decide to acknowledge and give recognition to the whistleblower for reporting a breach, with prior consent of the whistleblower

(including, but not limited to, expressing gratitude and public commendation by the top management).

WHAT IS RETALIATION AND HOW ARE WHISTLEBLOWERS PROTECTED AGAINST IT?

Prohibition of retaliation

Retaliation means any threatened, proposed or actual, direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the whistleblower. Retaliation may include, but is not limited to, the following: • suspension, lay-off, dismissal or equivalent measures;

- demotion or withholding of promotion; • transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference; • imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism, isolation;
- discrimination, disadvantageous or unfair treatment;
- disclosing the whistleblower's identity;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract; • harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

Aspöck has zero tolerance policy for retaliation. Any form of retaliation, including threats of retaliation and attempts of retaliation, are prohibited and must be reported immediately. Such reports may be submitted using Aspöck's whistleblowing solution, the mentioned e-mail adresses or also standard internal reporting channels.

Anyone engaged in retaliation may face serious internal - and potentially external - consequences under applicable legislation or regulations. If Aspöck identifies anyone involved in retaliation, these individuals will be subject to disciplinary action, which may include dismissal.

Action to deal with a whistleblower's own breach, wrongdoing, performance or management, unrelated to their role in whistleblowing, is not considered retaliation.

Protection against retaliation

Aspöck shall take all reasonable steps to protect whistleblowers from retaliation.

If it is established that retaliation is occurring or has occurred, Aspöck shall take reasonable steps to stop and address such conduct and support the whistleblower.

If remediation is required, Aspöck shall, to the greatest extent possible, restore the whistleblower to a situation that would have been theirs had they not suffered retaliation. For example:

- reinstating the whistleblower in the same or equivalent position, with equal salary, responsibilities, working position and reputation;
- fair access to promotion, training, opportunities, benefits, and entitlements; • restoration to the previous commercial position relative to the organization;
- withdrawing litigation;
- apologies given for any detriment suffered;
- compensation for incurred damages.

After a report is made the authorised staff shall make an assessment of the risk of retaliation against the whistleblower. Depending on the likely sources of harm identified through the risk assessment the authorised staff shall identify and implement strategies and actions to prevent such retaliation or contain identified retaliatory conduct to prevent further harm, for example:

- protecting the whistleblower's identity;
- sharing information on a strictly need-to-know basis;
- regularly communicating with the whistleblower;
- providing emotional, financial, legal or reputational support throughout the process;
- encouraging and reassuring the whistleblower of the value of reporting the breach and taking steps to assist their wellbeing;
- changing workplace or reporting arrangements;
- warning persons concerned or other interested parties that retaliatory conduct or breach of confidentiality can be a disciplinary offence.

The authorised staff shall monitor and review risks at various points in the process, such as when a decision is made to investigate, during the investigation into the report and once the outcome of an investigation is known, as well as, where appropriate, after the case has been closed.

The protections under this policy apply to the whistleblower even if the reported breach is not substantiated, if the whistleblower had reasonable grounds to believe that the information on the breach reported was true at the time of reporting. Also, whistleblowers who reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall qualify for the protection under this policy.

Any person who knowingly makes false reports shall be subject to disciplinary and/or other legal actions, which may include dismissal.

FOR HOW LONG ARE THE REPORTS RETAINED?

If a reported breach is not substantiated by the authorised staff and the respective data are not required by Aspöck for any further proceedings, the report and all the gathered information related to the report and its processing shall be permanently deleted 7 years after closing the case. If a reported breach is substantiated, the report and all the gathered information related to the report and its processing shall be stored for as long as necessary for the assertion and exercise of, or defence against respective legal claims.