

Keepit's Whistleblowing Policy

1. Overview

1.1 Introduction

A core value of Keepit is transparency and, with that, an open corporate culture, where everyone can freely express themselves if they have experienced any breaches or unlawful acts committed by the company's employees.

Acknowledging the importance of this type of information coming to light, this Whistleblowing Policy describes the Keepit whistleblowing scheme, incorporated in accordance with the Danish Whistleblower Protection Act (Lov om Beskyttelse af Whistleblowere, "DWBA") implementing the EU Whistleblowing Directive of 23rd October 2019.

By reporting breaches, whistleblowers play a key role in exposing and preventing serious breaches and safeguarding the welfare of employees, stakeholders, and business partners, as well as maintaining Keepit as an open and transparent company and avoiding circumstances that could adversely affect the company's reputation.

1.2 Purpose

The purpose of this Whistleblowing Policy is to explain the set-up for Keepit's Whistleblower Scheme; the whistleblower's rights (including for protection and anonymity), and the situations covered under the DWBA to stay compliant and prevent situations that are or might prove to be harmful to the company because these significant issues have not been reported and where employees, business partners, and others fail to report these significant issues and situations.

2. Scope of Application

2.1 Who can report?

The Keepit whistleblower scheme can be used by any person related to Keepit, including; current and former employees, consultants and private entrepreneurs, and interns whether remunerated or not; prospective employees who have not yet started their employment but who, during their employment process, has gained access to information which falls under section 2.2; business partners, hereunder suppliers and distributors; members of the Board and other stakeholders.

Employees in Keepit that have a concern are encouraged to discuss such matters first with their immediate manager or other appropriate personnel in Keepit. Where this is not possible the whistleblower scheme offers an alternative way of reporting.

2.2 What can be reported?

Keepit's whistleblower scheme can be used to report serious offenses, other serious matters, and violations of EU law that fall within the scope of the EU Whistleblowing Directive of 23rd October 2019.

This includes actions or omissions which are illegal or constitute a serious offense or breach within the areas listed below, and actions or omissions that enable bypassing a regulation within the areas stated below.

The report can include any information, hereunder reasonable suspicion, on actual or potential breaches and attempts to hide such breaches, which have taken place or are likely to take place, either within Keepit or elsewhere where Keepit was involved.

EXAMPLES

- Financial crime, including embezzlement, bribery, fraud, forgery, corruption, accounting fraud, and other breaches of competition law,
- Breaches of Keepit's Code of Conduct,
- Serious breaches of occupational health and safety and environmental regulations,
- Physical violence, harassment, and sexual abuse,
- Breaches which fall under the scope of the EU Whistleblowing Directive, hereunder:
 - Public procurement,
 - Financial services, products and markets, and prevention of money laundering and terrorist financing,
 - Product safety and compliance,
 - Consumer protection,
 - Protection of privacy and personal data, and security of network and information systems,
 - The free movement in the EU Internal Market, including provisions on state aid

Reports about the whistleblower's own employment are generally not covered unless it is regarding sexual harassment or other serious harassment.

Information about violations of internal guidelines of a less serious nature, such as rules on sick leave, clothing, and information on other personnel-related conflicts at the workplace, will not be regarded as gross violations and thus should not be reported to the whistleblower scheme. Such information may, in accordance with applicable guidelines, be submitted to the immediate manager or the HR department.

3. Rights and Protection

3.1 The Whistleblower

The Whistleblower Protection Act grants the whistleblower special rights that apply before, during, and after the person has submitted a report or disclosure.

A whistleblower is not considered to have violated any duty of confidentiality provided that the whistleblower has reasonable grounds (and is in good faith) to assume that the report was necessary to expose a situation encompassed by section 2.2.

Furthermore, a whistleblower cannot be punished for having gained access to reported or published information unless the act itself constitutes a criminal offense. The whistleblower cannot waive this protection either.

Protection against retaliation

The Whistleblower Protection Act protects all whistleblowers who report in good faith from retaliation, hereunder threat, or attempt of retaliation. Retaliation can be understood as any unfavorable treatment or consequence in response to an internal or external report or publication which causes or may cause harm to the whistleblower.

Keepit does not tolerate any form of retaliation against or punishment of persons who, in good faith, report or assist Keepit in investigating infringements under the whistleblower scheme. This includes suspension, termination, reprimands, retaliation, changed work assignments, changes to employee benefits, changes to reporting requirements, thwarting of the whistleblower's career prospects or reputation, threats to do any of the above, or deliberate omissions which may harm the person in question.

However, persons who knowingly and in bad faith report another person will not be protected. Persons who report other employees in bad faith may be subject to civil, criminal, and administrative sanctions as well as disciplinary sanctions, including dismissal.

Conditions for protection

Protection of the whistleblower is only applicable if the whistleblower had reasonable grounds to assume that the reported information was correct at the time of reporting *and* that the reported information falls under the scope of section 2.2.

3.2 Persons subject of the report

The person who is the subject of the report will be sent information about the suspicions which have been raised and reported. This includes information on i) his/her suspected conduct, ii) the departments in Keepit which might receive the report, and iii) how he/she should avail themselves of the right to respond.

All serious reports will be subject to thorough and confidential evaluation and investigation. Any misuse of the whistleblower scheme and any reports filed in bad faith will be sanctioned appropriately and all groundless reports will be dismissed and disregarded.

3.3 Personal data

All personal data being collected through or in connection with Keepit's whistleblower scheme will be processed in accordance with Keepit's [Privacy Policy](#).

Information collected in connection with a report submitted in the Keepit whistleblower portal shall be used for the investigation of the subject matter reported and shall not be used for a subsequent purpose not compatible with this purpose.

4. Anonymity and Disclosure of Identity and Confidentiality

4.1 Anonymity

Whistleblowers can provide their name or choose to report matters anonymously. The system makes it possible to have a dialogue with the whistleblower while still protecting his or her anonymity. However, Keepit encourages whistleblowers to provide their name in the report.

4.2 Disclosure of identity and confidentiality

Information on the identity of the whistleblower and other information from which the identity of the whistleblower can directly or indirectly be deduced can only be passed on to the persons responsible for handling the internal report. All persons who are involved in handling the report are bound by a special duty of confidentiality.

However, disclosure of identity can be allowed if Keepit is aware of the identity of the whistleblower. Under Danish law, we can and will in most cases be forced to disclose the name of the person to the individual who is being reported if the person so requests, or if the investigation leads to a police investigation or trial.

The person who is the subject of the report will only be sent information as stated in section 3.2. No information will be provided on who has submitted the report, even if the whistleblower has chosen not to remain anonymous. However, if a non-anonymous report results in legal proceedings being initiated against the reported person, the person in question risks being called as a witness in the proceedings.

5. Process

5.1 Technical set-up and security

The Keepit whistleblower portal is hosted by the independent third-party, EQS Group A/S, which guarantees anonymity, security, and a user-friendly system.

The whistleblower portal can be found at: <https://keepit.integrityline.com/frontpage>

When submitting a report, you will be asked to choose between providing your contact details or stay anonymous. If you choose to report anonymously, you will be asked to choose a password. You will then receive a notification of receipt and a unique case ID. To log on to the system to follow your case, please insert your password (the password you used to create the case) along with the case ID. If you have provided your email address chosen to be notified of any changes, you will receive an automatic notification to your email whenever there are any developments in the case.

All data transmission between the internet browser and the database is encrypted in accordance with the industry standards applicable at all times for cryptographic technologies.

5.2 Communication and Procedure

When submitting your report, you will receive an automated confirmation of receipt.

Within 3 months from the date of the receipt, you will receive detailed feedback on your report.

If further information on the report is needed, you will be contacted through the whistleblower portal. You are also allowed to update or rectify your report if you have additional or updated information relating to the submitted report.

5.3 Assessment of the report

If the whistleblower's report concerns matters that fall within the scope of the whistleblower scheme, the General Counsel and HR Manager will make an initial assessment of the report, including the possibilities for shedding sufficient light on the matter. If the nature of the report does not preclude this, the report will be handled solely by the General Counsel. If the nature of the report prevents the case from being handled by the General Counsel, it will be exclusively handled by the HR Manager.

If the information falls within the scope of the whistleblower scheme and relates to a qualified and verifiable matter, i.e., a matter which can be considered to be serious, of significant importance or of a recurring nature, and if it is deemed that it is possible to shed sufficient light on the matter, the matter will be further investigated in detail by the General Counsel.

The investigation should draw on all relevant information including but not exhaustively statements from the person to whom the report relates, relevant documentation, interviews with other employees etc. If deemed relevant, external assistance may be brought in for conducting the further investigation.

5.4 Conclusion of the report

Based on the investigation, a decision will be made as to whether the case is unfounded, or whether the employee who has been reported should be issued with a warning or be dismissed, or whether the case, if criminal, should be reported to the police.

If the report contains information on matters that fall outside the scope of the whistleblower scheme, or if the report is considered to be unfounded, it will be rejected.

If the report concerns matters which are found not to be serious, of significant importance or of a recurring nature, or if it is not possible to shed sufficient light on it, the report will be dismissed.

6. Questions

Questions regarding the Keepit whistleblower scheme in general can be addressed to the General Counsel, Mikkel Banskolt Oxfeldt, at mox@keepit.com. Questions regarding how personal data is handled contact dpo@keepit.com.