



Kempinski Global Whistle Blowing Policy

15 June 2023 – V2

A. What is the purpose of the Whistle Blowing Policy?

1. The purpose of this Whistle Blowing Policy is to encourage all employees to communicate concerns regarding ethical and professional wrongdoing within the organisation and to clarify when and how to communicate these concerns. Kempinski reassures employees that you can raise genuine concerns regarding ethical and professional violations without fear of reprisal.
2. Kempinski is dedicated to operating at the highest standards of ethics and integrity and to maintaining a transparent and conducive working environment. Compliance with laws, as well as internal and external rules and regulations is fundamental to our business conduct and the basis for the trust of our guests. Details regarding your responsibilities to maintain such ethical standards are described in our Code of Conduct and Business Ethics (“Code of Conduct”). The Code of Conduct can be found on the intranet and HR Department responsible for the property / office where you work and is provided to new employees with their on boarding material.
3. Kempinski considers employees (identified as staff of hotels operated by Kempinski, as well as Kempinski employees at a corporate and regional level) raising concerns to be a positive act that can make a valuable contribution to improving our organisation's long-term success as well as enhancing the environment for employees and guests. The Policy applies to all employees, regardless of their level of seniority or function within the organisation.
4. This Policy and other policies described in the Employee Handbook complement each other and exist in parallel to address different requirements. This Policy does not replace other policies but rather focuses on different areas and provides an alternative channel to communicate concerns.
5. The Whistle Blowing channel covered in this policy will also be made available to outsourced employees of subcontracting companies working on the premises of Kempinski hotels.
6. Kempinski remains committed to and encourages direct communication between staff and line and senior managers on-site at every property and in every corporate and regional office. All managers and supervisors are expected to listen to employee concerns, encourage their input, and seek resolutions to problems.
7. Finally, whistle blowing schemes must be implemented in compliance with EU data protection rules, namely the General Data Protection Regulation. As a matter of fact, the implementation of whistleblowing schemes will in the vast majority of cases rely on the processing of personal data (i.e. on the collection, registration, storage, disclosure and destruction of data related to an identified or identifiable person), meaning that data protection rules are applicable.

Personal data is defined as any information that relates to an identified or identifiable natural person. Personal information does not only include information about an individual's private life and family life, but also information regarding an individual's activities, such as his or her working relations and economic or social behaviour. The application of these rules will contribute to the proper functioning of this whistle blowing scheme.

B. What is the definition of Whistle Blowing?

8. Whistle Blowing describes the process during which an employee communicates concerns through a formal and confidential channel that violations of ethical standards have taken place within an organisation. Wrongdoing may include illegal behaviour or financial malpractice or dangers to the public or to the environment (for further detail on the types of wrongdoing, please see Section C in this Policy).
9. It is important that our employees promptly raise concerns regarding illegal or unethical activities within the organisation so that Kempinski is alerted to any such instances as soon as possible, so that they can be addressed as quickly and efficiently as possible. Employees are often the first to realise that a violation of our usual standards and Code of Conduct may have occurred. The use of the system is entirely optional and voluntary and employees who do not use the system will not suffer any adverse consequences either for using or for not using it.

C. When should I consider using the whistle blowing channel?

10. This Policy is intended to facilitate the transmission of issues of concern regarding breaches of our Code of Conduct and Business Ethics. Ideally, concerns are often addressed most effectively at a local level – through line managers or HR, Department Heads, or the Hotel Manager (or Number 2 equivalent) or General Manager. However, there may be scenarios in which you do not feel comfortable addressing concerns through direct interaction with your line manager or the hotel management, and the matter in question is serious enough to warrant the attention of Kempinski's staff outside the property where you work. Such scenarios can be addressed at a regional and corporate level through this policy.
11. The Policy will allow employees, if they wish to do so, to report concerns, questions and issues under applicable rules for the matters listed below. Please note however that this policy is intended to cover concerns which are in the public interest only and may at least initially be investigated separately but might then lead to the initiation of other procedures (e.g. disciplinary). These concerns include: criminal offences; breach of any legal obligation; miscarriages of justice; danger to the health and safety of any individual; damage to the environment; or the deliberate concealing of information about any of these. The disclosure can relate to current incidents, events in the past, or situations that could occur in the future.
12. This Policy is intended for the following type of incidents:
 - Fraud and financial irregularity
 - Bribery and corruption

- Management conflict of interest
- Procurement fraud
- Misuse of hotel assets
- Harassment and intimidation
- Discrimination
- Commissioning of a crime, direct and indirect involvement in a crime
- Failure to comply with local regulations and legal obligations
- Danger to health and safety
- Disclosure of confidential information
- Misuse of company data
- Misuse of social media
- Failure to comply with Intellectual Property protection
- Mishandling crisis management
- Abuse of power leading to abuse of employees, clients, guests and suppliers
- Coverage of other employee's wrongdoings
- Business negligence
- Other improprieties and violations of our Code of Conduct.

Please note that if the incident represents a clear and present danger to people and assets you should immediately alert the General Manager, Hotel Manager (or Number 2 equivalent) and/or police for immediate action. The Whistle Blowing Policy is not intended to respond to incidents that require immediate attention. In such cases, it is the obligation of the General Manager or Number 2 at hotel level to immediately inform the regional office and the regional office to inform the corporate office without delay. For Corporate or Regional Office Employees, such cases should be immediately and directly communicated to the Chief Executive Officer, Chief Human Resources Officer or regional Chief Operating Officer.

13. The Policy is **not intended** for the following type of incidents:

- general complaints – e.g. personal grievances about pay, compensation, working conditions or personal treatment by colleagues or supervisors unless the issues are significant in nature and the individual does not feel comfortable to escalate them to the General Manager of the property / Vice President of the department he/she is working for, nor to the respective local HR department.

- communication of concerns about violations of ethical standards that are minor in scale or impact – in such cases the main channels to use are the ones described in the local grievance policy, typically the line manager, Department Head, HR department, Hotel Manager / Number 2, or General Manager / in case of the regional and corporate office the senior leader in charge of Regional Operations or respective (Senior) Vice President in question as well as the HR department. If the employee is raising issues which implicate some or all of the positions mentioned above and does not feel comfortable raising such concerns through direct interaction with local management, (s)he may also use the whistle blowing mechanism.
- Issues that arise from error or incompetence.
- To question business decisions unless there are concerns regarding wrongdoing in relation to these decisions.
- Guest complaints in the ordinary course of business.

D. How do I raise a concern?

14. Kempinski has associated with Deloitte, who is a recognised global provider of independent whistleblowing solutions to corporate and public sector entities across the globe. The new Kempinski Speak Up platform is a digital whistleblowing solution, powered and managed by Deloitte that equips our organisation with secure and confidential reporting channels.

You can log a disclosure / suspicion via the Kempinski Speak Up platform at the below URL:

[Kempinski Speak Up \(deloitte-halo.com\)](https://deloitte-halo.com)

For China only, please use the below URL:

[凯宾斯基举报服务 \(tip-offs.com.cn\)](https://tip-offs.com.cn)

15. This service is **confidential**, and you will not be required to reveal your identity unless you choose to do so. Personal details and information provided to Kempinski Speak Up may be disclosed to law enforcement agencies or regulatory authorities, as required to meet applicable, laws, rules and regulations.

There are three types of Disclosure Security:

- Confidential but not Anonymous – Your personal details will be disclosed in the report to Kempinski Group, entities, offices and hotels
- Confidential (Restricted) – Your personal details will only be disclosed to Deloitte but will not be disclosed in the report to Kempinski Group, entities, offices and hotels
- Completely Anonymous – You will remain completely anonymous, although you are encouraged to identify yourself as this frequently makes the investigation and resolution process easier.

You will also be required to indicate your location (region) and disclosure type that best describes the issue you are reporting.

16. To effectively address any issue regarding violations of ethical standards, we require as much detail as possible in order to understand what has occurred and facilitate any subsequent action or investigation. The following information is critical to include in your report:

- What is the issue you wish to report? (Full description)
- Who was involved? (Name/Position)
- Were there any witnesses? If so, who? (Name/Position)
- When did this occur? (Exact Date/Time, Work/After Hours)
- Where did the incident take place? (Company Premises, Social Event)
- Has this occurred before? (Frequency, Period of Time)
- Is there any physical documentation or evidence? (If so, what)
- Have you informed anyone or reported the incident internally, if so to whom and when?
- Are you or any other person in physical danger?
- Your relationship to company.

You will also be able to add attachments that you feel may help inform this disclosure, taking care not to include information that may reveal your identity if you wish to remain anonymous.

If you feel comfortable expressing your concerns in English, please do so. If not, please feel free to write in your preferred language and the recipient will procure a translation. If you have a person of trust who can translate for you, you can also ask this person to communicate on your behalf.

17. Please note that no sensitive personal data may be disclosed while reporting. If such data is given in a procedure of raising and notifying the concern, Kempinski will not record such data or destroy the carrier of such data immediately. In rare cases when sensitive data is of key importance for the proceedings, Kempinski will inform the person who raised concern and provided Kempinski with such data, that the data are regarded as sensitive and will be therefore processed solely for the purposes of the proceedings on the basis of relevant local legal provisions and this Policy. Sensitive personal data includes personal data revealing or relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

E. Who has access to personal data and reporting lines?

18. Procedure between Deloitte and Kempinski:

- A Deloitte analyst assigned to Kempinski Speak Up will review the information you have given, summarise the information provided, suggest specific follow-up action and submit a report to designated Kempinski representative(s) for follow-up or corrective action
- The designated Kempinski representative(s) discuss content and possible investigation approach with the respective senior leader in charge of Regional Operations
- Kempinski will then decide what action to take

19. Personal data will be disclosed only to the following authorized persons on a need-to-know basis:
- persons working for your employer (relevant Kempinski Group company) and for Kempinski Hotels S.A. involved in the processing of alert or concerns raised in the whistleblowing procedure
 - other instances if legally required; necessary to protect our legal rights.
20. If you feel comfortable expressing concerns regarding violations of ethical standards to the local management, then please consider doing so first. Communications through the Kempinski Speak Up platform that express legitimate concerns about violations of ethical standards will only be sent to the Regional Office (received by HR and investigated by the respective functional departments, e.g. Finance, Operations, HR) and copied to heads of the corporate HR and Legal departments at the corporate office in Geneva. Local management will not be included in the distribution of your report.
21. For any of the following cases, the Chief Human Resources Officer and General Counsel must be involved from the start, to ascertain the required involvement of corporate departments in the investigation process and inform all members of the Management Board. Moreover, in these cases, the CHRO will inform and involve the Audit & Compliance Committee:
- cases involving a General Manager / Hotel Manager or Number 2
 - cases involving any other HOD or ExCom member at the hotel or regional /corporate level
 - cases which could have an impact of brand reputation
 - cases which could damage owner relationships
 - cases with a potential financial impact of more than €5,000.

At the corporate office, the Chief Human Resources Officer, General Counsel and the Head of Internal Audit will receive the whistleblowing email and involve other departments, such as Finance or Operations, to investigate where appropriate. The cases involving Regional or Corporate Vice President level and above will be reported to the Audit & Compliance Committee.

Further, as detailed below in subsequent sections, your identity will not be disclosed to the hotel or office where you are employed, unless you authorise it.

If you would like to speak to someone of your choice within Kempinski, please mention the name of the individual in your report.

F. What will happen to me if I raise a concern?

22. The decision to communicate violations of ethical standards may involve overcoming initial hesitations or doubts regarding whether or not to speak up. Management will not retaliate against any employee as a result of raising legitimate concerns (including, but not limited to failure to promote, denial of training, blocking access to resources, suspension, re-location, disciplinary sanction, dismissal, etc.). Kempinski is committed to supporting all staff in Kempinski branded hotels and we are sensitive to your concerns.

23. All reports under this Policy will be promptly and appropriately investigated by specifically trained personnel of Kempinski and all information disclosed during the course of the investigation, including the identity of the employee who reported a suspected violation, will remain confidential, except as necessary to conduct the investigation and take any remedial action, in accordance with applicable law. The identity of the whistle blower will not be communicated to the person who was reported against, unless there is permission to do so from the individual raising the complaint.
24. We will take appropriate disciplinary action against any employee who attempts to bully or harass another employee who has reported a violation in good faith.

G. What will happen after I raise a concern?

25. We will acknowledge receipt of all concerns that are communicated through this reporting channel, and you will receive a reference number. You can perform a Disclosure Follow Up directly on the Kempinski Speak Up platform by using this reference number.
26. Once you have made your report, you will not need to be involved in the report any further. However, if you have new or additional information, or would like to make an adjustment to a previous report, you can log onto the website with your reference number and password provided when you submit your initial report. Alternatively, you can contact the service and quote the reference number.
27. Upon receiving the concern, launching an investigation depends on a number of factors including the information provided, the details, documentation and Kempinski Group, entities, offices and hotels company policy. Kempinski Group, entities, offices and hotels will decide what action is required when they receive the report.

We may also reply and seek to contact you to help us understand the matter in more detail.

28. Kempinski is fair to all its employees, including those who may be mistakenly or wrongly accused of wrongdoing. As a result, please be aware that raising a concern may not automatically or necessarily result in an investigation being conducted.
29. We will deal with all concerns that are communicated through the whistle blowing channel fairly and equitably.
30. After assessing the most effective course of action, we may update you regarding what action has been taken – or not taken and why. The nature of concerns can vary significantly, as does the resulting action that is taken. Therefore, there is no specific timeframe and will depend on the circumstances of the enquiry we might undertake.
31. All documents related to reporting, investigation and enforcement pursuant to this Policy shall be kept in accordance with the Company's record retention policy and applicable law. Reports and any personal data involved must be destroyed or archived 2 months after the end of any internal investigation or after the end of any disciplinary or judicial proceedings relating to the whistleblowing report. Reports that are out of the scope of the whistleblowing system must be deleted or archived without delay.

H. Can I raise a concern anonymously?

32. European data protection law recommends that employees should identify themselves when they raise concerns, unless there are exceptional circumstances which require an anonymous reporting or if applicable laws allow anonymous reporting. This is to avoid abuse of the procedure and to allow a fair proceeding. The identity of employees who raise concerns will not be disclosed to individuals who are implicated in suspected violations of our ethical standards.
33. Our assessment of concerns that are communicated through this Policy is based on content of the communication, not the identity of the employee. However, employees who identify themselves add credibility to the concerns they raise and enable us to communicate with them more effectively, which increases our effectiveness in addressing their concerns.
34. To the extent permitted by applicable laws, you are allowed to submit an anonymous report, especially if you have valid reason to believe that our guarantees to keep your identity confidential would not be effective. Anonymous reports are dealt with special precautions such as a preliminary review by the recipient of such report to assess whether it should be considered or not, including the fact(s) why you think the anonymous reporting is valid.
35. If you wish to stay anonymous, we will not disclose your identity if it is not required by law. There may be cases when disclosure of your identity is a key factor in the proceedings (i.e. witness evidence in court proceedings). In such instances, we will discuss with you possible actions. Also, if you do not tell us who you are we will not be able to protect your position or to give feedback on how the matter was dealt with. In exercising your right to stay anonymous, the factors to be taken into account would include:
 - how serious is the issue raised,
 - how credible is your concern,
 - how likely it is to confirm the concern on the basis of other sources.

I. What about concerns which are unfounded or malicious?

36. No retaliation or disciplinary action will be taken against any employee who raises an issue of concern in good faith – even if the issue of concern turns out to be unfounded or incorrect.
37. We will carefully and objectively analyse the content of communications we receive. However, we emphasise that allegations sent will not automatically be investigated; any decision to investigate will follow an independent assessment in which we consider investigation to be the appropriate course of action. If we consider there to be insufficient basis to launch an investigation based on the information provided, we may not initiate an investigation – so please ensure that communications contain as much detail as possible. Disciplinary action may be taken against an employee who has made an allegation maliciously or for personal gain.

The following examples provide indications of which types of issues may be most effectively covered by which policy.

- EXAMPLE: “A colleague has repeatedly received favours including cash and cases of alcohol from one of the third-party vendors. I suspect my Department Head knows about it and may be involved.”

Policy: Whistle Blowing

Due to the suspicion that the Head of Department may be colluding in wrongdoing, it is not appropriate to address this matter with the Head of Department. Concerns regarding this type of violation may be addressed most effectively by raising the issue directly with the General Manager, Hotel Manager and/or HR in the first instance.

Or, if additional factors make an employee uncomfortable doing so, using the dedicated whistle blowing email address mentioned in this policy may be an appropriate mechanism to communicate these concerns.

- EXAMPLE: “My line manager treats me unfairly and is rude towards me.”

Policy – Direct Interaction with Line Manager or Local Management

Although this issue can have a significant impact on morale and performance, it should be addressed in the majority of cases by raising it with your line manager or local management, including General Manager, Hotel Manager or local HR. Please refer to the grievance policies contained in the Employee Handbook.

The more information and detail that you provide, the better our understanding of the issues of concern will be, which will make us better equipped to address your concerns. We understand that you may not remember every specific detail – but the more detail you are able to provide, the more effectively we can respond to address your concern.

- ✓ Example of good level of detail:

“On 1 March 2016, the Finance Manager, “John Doe”, stole three laptops from the IT office. “John Doe” walked out of the staff exit at 10.15 pm with the laptops in his hand, and drove home. Two waiters, “Tom Jones” and “Mary Miller”, witnessed him do this. When “Tom Jones” asked “John Doe” what he was doing, “John Doe” threatened him. The General Manager is aware of this theft, but has not taken any action.”

- ☒ Example of vague level of detail.

“The IT Manager is stealing from the organization. He stole something earlier in 2016. He has threatened other members of staff. No one likes him. Everyone is scared of him.”

J. Rights of employees using the whistle blowing channel and of persons on whom a report is made

38. The accused must be informed about the processing of his personal data (categories of data, purpose of gathering, processing and storing, identity of the entity responsible for the processing) and may also request such information (cf. below). However, this does not apply where the data must be kept secret because of prevailing interests of a third party. Such information can be withheld at least until the end of the investigation if the purpose of the investigation would be undermined otherwise.

39. In accordance with applicable data protection and privacy laws, employees using the whistle blowing channel and persons on whom a report is made as well as any person whose data are collected in the context of a report, have the right to access and correct their personal data that are processed and to object upon legitimate grounds to the processing of their personal data.

K. How is personal data kept secure

40. Kempinski and its processors maintain appropriate organizational and technical safeguards to protect your personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, use, and all other unlawful forms of processing of your personal data in our possession.

41. We use a variety of security measures to secure your personal data, ranging from measures that are organizational (such as a security policy and monitoring assigned authority); technical (such as using passwords to protect documents, login and password protection of workstations); and physical (such as burglary alarm).

42. The transfer of your personal data outside the European Economic Area (EEA) and outside China is subject to restrictions. Kempinski has taken steps so that your personal data are subject to an adequate level of protection at all Kempinski locations.

In order to legitimize the transfer of your personal data outside EEA, we conclude a data transfer agreements in accordance with the relevant EU Standard Contractual Clauses.

Reports including personal data of individuals in China will be transferred to third countries after being anonymised or only if Kempinski and its processors can rely on one of the data transfer tools released by the Chinese authorities.

43. Third party data processors may only process your personal data if they are held by contractually binding security and confidentiality safeguards, in accordance with the applicable data protection legislation.

L. Which entities are covered by this Policy

44. This Policy covers the Kempinski Group (Kempinski entities and Hotels operated by Kempinski - more information in regard to the list of the Kempinski operated hotels can be found at the following [link](#)).

M. How is the policy changed

45. We may alter this Policy. If changes are made to this Policy, the updated version of Policy will be made available to employers before the changes are effective. Each employee may obtain a copy of the updated Policy upon request.

46. This Policy is effective immediately and replaces any previous versions.