



Design Management S.r.l.
WHISTLEBLOWING PROCEDURE
PURSUANT TO LEGISLATIVE
DECREE 24/2023

DESIGN | MANAGEMENT | SRL Unipersonale

Società facente parte del Gruppo Kering

soggetta ad attività di direzione e coordinamento di KERING HOLLAND NV, società di diritto olandese con sede in Amsterdam

Sede Legale via San Paolo, 7 20121 Milano (MI)

Capitale sociale euro 10.646,00 i.v. reg. imprese cciaa. di Milano e cod. fisc. e part.iva 05063610488

1. Kering Code of Ethics
2. Kering Anti-Corruption Policy
3. Kering Compliance Manual
4. Kering Gifts, Hospitality, and Entertainment Procedure
5. Kering Donations and Sponsorship Procedure
6. Kering Conflicts of Interest Procedure
7. Kering Sanctions Procedure
8. Kering Third Party Due Diligence Procedure
9. Kering Interacting with Public Officials Do's and Don'ts
10. Kering Human Rights Policy

1. Introduction	4
2. Definitions	4
3. Issuing an Alert: Eligibility and Requirements.....	6
4. Reporting an Alert: Process.....	9
5. Contents of the Alert.....	9
6. Reception and Management of the Alert	9
7. Identity of the Reporting Party and Confidentiality Requirements	12
8. Prohibition of Retaliatory and/or Discriminatory Acts	12
9. External Reporting.....	13
10. Processing of personal data	14

1. Introduction

This Whistleblowing Procedure (the “Procedure”) describes the existing system within the Company in order to report the conducts defined below and to organize the collection and verification of all such alerts.

The implementation of this Procedure involving the processing of personal data has been established in compliance with the General Data Protection Regulation, EU Regulation 2016/679 (the “GDPR”) and with applicable law regarding the processing of personal data. If you would like to obtain further information on the collection and processing of personal data, please contact the DPO: dpo@themall.it.

Resorting to an alert according to this Procedure (hereinafter the “Alert”) is optional, no penalty will be incurred in the event of non-use.

This Procedure is the only procedure applicable within the Company. It cancels and replaces any former version.

2. Definitions

Alert:	A report made by a Reporting Party for which the purpose is to supply the Compliance Officer of information obtained in the course of professional activities of which the Reporting Party has personal knowledge pertaining to actions or conducts that have occurred or are very likely to occur and that are deemed by the Reporting Party to constitute a Breach (see definitions and Section 3 below).
Reporting Party:	Any individual(s) who report(s) an Alert and is (are) entitled to do so, in application of Section 3.
Whistleblowing hotline:	the IT platform, provided by a qualified external IT service provider, designated by the Company to receive and forward Alerts to the Compliance Officer, as specified in Section 4 below.
Kering Group:	all entities (including the Company) that are directly or indirectly controlled by the French company Kering SA, with registered office in 40 rue de Sevres – 75007 Paris – France.
Company:	Design Management S.r.l., with registered office in Via San Paolo 7, 20121, Milan, VAT Number 05063610488.
Referenced Individual:	Any person(s) other than the Reported Individual mentioned in the Alert by the Reporting Party.

DESIGN | MANAGEMENT | SRL Unipersonale

Società facente parte del Gruppo Kering

soggetta ad attività di direzione e coordinamento di KERING HOLLAND NV, società di diritto olandese con sede in Amsterdam

Sede Legale via San Paolo, 7 20121 Milano (MI)

Capitale sociale euro 10.646,00 i.v. reg. imprese cciaa. di Milano e cod. fisc. e part.iva 05063610488

- Reported Individual:** Any person(s) referred to in the Alert as having participated in behavior or actions that are the subject of the Alert.
- Compliance Officer:** the individual entrusted with the responsibility to receive the Alerts and handle the investigations within the organization of the Company.
- Breach:** Conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity and consisting of:
1. administrative, criminal, civil and accounting infringements, that do not fall under numbers 3), 4), 5) and 6) referred to in Art. 2, para. 1 of Legislative Decree 24/2023);
 2. unlawful conduct relevant under Legislative Decree 231/2001, or violations of the Organizational Model adopted by the Company, as well as of the Kering Group's Code of Ethics and Code of Conduct and under internal regulations (procedures, policies, etc. e.g. relating to (i) bribery and corruption, (ii) human rights, (iii) fraud, (iv) conflicts of interest, (v) competition law, (vi) trade sanctions and export control, (vii) money laundering) of Kering Group and of the Company (which do not fall under numbers 3), 4), 5) and 6) referred to in Art. 2, para. 1. Of Legislative Decree 24/2023);
 3. offenses that fall within the scope of the European Union or national acts indicated in the Annex to Legislative Decree 24/2023 or national acts constituting implementation of the European Union acts indicated in the Annex to Directive (EU) 2019/1937, although not indicated in the Annex to Legislative Decree 24/2023, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
 4. acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in relevant secondary legislation of the European Union;
 5. acts or omissions affecting the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including violations of the Union's competition and state aid rules, as well as violations affecting the internal market related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
 6. acts or conduct that frustrates the object or purpose of the provisions set forth in Union acts in the areas indicated in numbers 3), 4) and 5) in Art. 2, para.1. Of Legislative Decree 24/2023.

3. Issuing an Alert: Eligibility and Requirements

This Procedure applies to:

- members of staff, persons whose employment has ended when the information has been obtained within the framework of this relationship, and job applicants when the information was obtained as part of an application process;
- self-employed workers, freelancers, contractors, subcontractors, consultants, volunteers and interns (including unpaid), who work or have worked at the Company;
- shareholders and partners;
- members of the board, of the management or of a supervisory body of the Company;
- in general, all those who, although not belonging to the Company, work or have worked directly or indirectly for it (e.g., suppliers of goods and services) and/or on its behalf (e.g., agents, distributors, business partners, etc.);

("Covered Persons").

All Covered Persons above are entitled to send an Alert to the dedicated recipients provided that the purpose of the Alert is to provide information regarding a Breach (see definition above).

Alerts should not include any information the disclosure or dissemination of which would contravene the rules regarding the protection of defense secrecy, medical secrecy, secrecy of judicial deliberations or attorney-client privilege.

The Reporting Party must act in good faith and cannot be directly financially compensated for having reported an Alert.

Reports must be made in a disinterested manner and in good faith: reports provided for the mere purpose of retaliation or intimidation, or ungrounded reports made with willful misconduct or gross negligence shall be sanctioned. In particular, sending of any communication that proves to be ungrounded on the basis of objective elements and that is, again, on the basis of objective elements, made for the sole purpose of causing unjust damage to the Reported Individual, shall be sanctioned.

Figure 1: Non-Exhaustive Illustrations of Behaviors that Could Constitute an Alert

Definition	Examples
<p>Corruption</p> <p>Whenever someone unduly offers or promises – directly or indirectly – any form of benefit (including gifts, money, etc.) to someone else, so that the recipient of the benefit does or refrains from doing something in the context of his/her professional activity or for the exercise of its functions or powers.</p> <p>The notion of corruption applies both to:</p> <p>(i) People working in the public sector, such as those who have been elected to public office; and</p> <p>(ii) People working in the private sector.</p> <p>The “corruption” can be active (<i>i.e.</i>, the person proposing, offering, or promising) or passive (<i>i.e.</i>, the person accepting the promise or the offer). Both behaviors may be prosecuted by authorities.</p>	<ul style="list-style-type: none"> • Paying a bribe to a custom officer to ensure that he or she releases a shipment quicker. • Accepting a free vacation offered by a supplier as a reward for having placed an order with that supplier. • Inviting a buyer at a distributor’s as well as his/her spouse/partner to stay, for example, at a luxury hotel so that better sales terms and conditions can be agreed on.
<p>Theft</p> <p>The fraudulent removal or appropriation of property belonging to another person without his/her permission or consent.</p>	<ul style="list-style-type: none"> • Removing products from stock.
<p>Sexual Harassment</p> <p>Repeatedly subjecting a person to sexually connoted comments or behavior that are detrimental to the person’s dignity due to their degrading or humiliating nature or creating an intimidating, hostile or offensive situation for him/her.</p>	<ul style="list-style-type: none"> • Making comments about his/her anatomy. • Attempting to obtain sexual favors. • Taking professional retaliatory measures. • Sending erotic photos.

<p>Sexual harassment is also when the same employee suffers such comments or behaviors coming from multiple people, concerted or at the instigation of others, regardless of whether each of these individuals have not repeatedly engaged in the act or if the comments or behavior successively come from multiple people who, without doing so together, know that these comments or behavior are repeated.</p> <p>Any form of serious pressure, even if not repeated, exercised with the real or apparent aim of obtaining any act of a sexual nature, regardless of whether it is sought for the benefit of the author of the facts or a third party, constitutes sexual harassment.</p>	<ul style="list-style-type: none"> • Having an insulting behavior towards a colleague that consists of insults and remarks of a sexually loaded nature and inappropriate gestures.
<p>Sexist Conduct</p> <p>Any act linked to the sex/gender of a person aimed at or resulting in attacking that person's dignity or creating an intimidating, hostile, degrading, humiliating or offense environment.</p>	<ul style="list-style-type: none"> • Making sexist comments, including sexist jokes. • Showing signs of incivility, such as giving nicknames to colleagues in relation to their sex/gender, ignoring legitimate requests from a colleague related to his/her sex/gender, addressing colleagues in unprofessional and infantilizing terms. • Only valuing a colleague by praising the qualities linked to his/her gender.
<p>Moral Harassment</p> <p>Repeated acts towards a colleague, the purpose or outcome of which is a deterioration of the colleague's working conditions that could lead to violating his/her rights and his/her dignity, to altering his/her physical or mental health, or to compromising his/her professional future.</p>	<ul style="list-style-type: none"> • Humiliation • Degradation • Bullying or unjustified critiques • Oppressive measures • Aggressiveness • Isolation • Unjustified disciplinary pressure

4. Reporting an Alert: Process

The Alert shall be reported:

- through the Whistleblowing Hotline accessible by typing in the following url: wb.themall.it;
- through the recorded voice message system, available on the Whistleblowing Hotline;
- at the request of the Reporting Party, orally through a face-to-face meeting with the individual(s) responsible to handle the Alert pursuant to section 6 below, which can be requested through the Whistleblowing Hotline, and must be scheduled within a period of 20 business days following his/her request. Full confidentiality of the meeting will be ensured;

An acknowledgement of receipt will be sent within 7 days.

The Alert shall be processed by the Compliance Officer and it shall receive full guarantees of the impartiality, expertise and confidentiality needed to investigate it. Indeed, the Compliance Officer benefits from specific, in-depth trainings and dedicated resources and have a duty to reinforced confidentiality. Moreover, the Compliance Officer is required to carry out investigations or inquiries in total independence and confidentiality.

On his or her end, the Reporting Party commits to respect confidentiality during the submission of the Alert.

5. Contents of the Alert

All Alerts must be worded in such a way to be objective and sufficiently detailed. The Alert should include the following:

- the identity, title and contact details of all Reported Individuals or Referenced Individuals;
- the identity, title and contact details of the Reporting Party(ies) of the Alert (except if the Alert is anonymous – see paragraph 7 below for the relevant details);
- a description of the facts reported;
- the supporting document(s) to substantiate the facts reported (in any form or medium whatsoever).

Value judgments and subjective comments regarding individual's behavior will not be considered and should not be included in the Alert, which should remain factual and should only contain information directly related to its subject.

To the extent possible, the facts should be presented clearly, succinctly, and exhaustively.

6. Reception and Management of the Alert

The Alert is received by using one of the methods described in Section 4 above. Within the organization of the Company, the Alerts will be managed by the Compliance Officer.

If the Alert refers to the Compliance Officer, the Company will identify other individual(s), not in conflict, to handle the investigation.

Any Report received by a person other than those identified above (e.g., by the hierarchical superior of the Reporting Party) and/or through channels other than those indicated in Section 4 above, must promptly be forwarded to the Compliance Officer within 7 days of its receipt, if it is clear from the Alert or the recipient can reasonably deem that the Reporting Party's intention was to issue an Alert under this Procedure and to benefit of the guarantees offered by the Legislative Decree No. 24/2023 and by this Procedure. In case the Alert is transmitted to the Compliance Officer by the recipient, the Reporting Party shall be simultaneously informed.

Once received by the Compliance Officer, firstly, the Alert is analyzed to verify if it meets the conditions set forth in Section 3. For this purpose, the Reporting Party may be asked to provide additional information.

Authorization to access the Alerts is limited to the Compliance Officer and to those specifically authorized in writing by the Compliance Officer in order to provide assistance in the management of the Alert (e.g. other Company or Group functions; external consultants), provided that confidentiality requirements and obligations are extended to them. Access is subject to traceability procedures.

Following the receipt of the Alert, the Compliance Officer will assess the significance of the allegations, deciding either:

- to dismiss the Alert if it does not meet the conditions set forth in Section 3, and/or if, after verification, it appears that the alleged facts do not fall within the scope of application set forth in Section 3 and/or do not constitute any of the situations listed in Section 3. In such a case, the Reporting Party is informed of the reasons why the Alert has been dismissed; or
- to verify the facts, either themselves or by entrusting this task to a restricted number of individuals under their supervision – including the Human Resources Department, the Group Internal Audit Department, the Finance Department, the Tax Department, or the Compliance Officers of Kering or of the entities of the Kering Group - who will ensure that the verifications are conducted fairly, timely and appropriately.

All the subjects involved in the management of the Alert must observe the requirements of confidentiality set forth in Section 4.

If, following a preliminary analysis, the Compliance Officer deems the Alert to concern violations or alleged violations of the Organizational Model, or the commission of violations relevant under the Legislative Decree No. 231/2001, he/she shall inform the Supervisory Body of the Company through a dedicated communication in which the relevance of the reported facts under the Legislative Decree No. 231/2001 will be highlighted, in order to allow the Supervisory Body to take all the appropriate actions pursuant to the Organizational Model.

The facts described in the Alert will be first analyzed so that the Compliance Officer can (i) gain an

understanding of their context, (ii) determine whether immediate action should be taken to prevent imminent harm to people or property, to avoid further non-compliance or to preserve documents or information and to make every effort so that no retaliatory action is taken against the Reporting Party and/or the individuals involved and (iii) plan the schedule and overall plan for verifying the facts, including via an internal investigation. As part of the internal investigation, the Compliance Officer may carry out any activity deemed appropriate, including the personal hearing of the Reporting Party and any other person who can provide information on the reported facts and the examination of documents/e-mails, in compliance with the current legislation on the protection of personal data. The Compliance Officer may also make use of technical advisors (such as external professionals or internal specialists of the Company or the Kering Group).

The Reported Individual may be heard, or, at his or her request, must be heard, including by means of a paper procedure through the acquisition of written comments and documents.

Reporting Party(ies) should, to the extent possible, cooperate to comply with any reasonable request to clarify facts and/or circumstances and provide (additional) information. To this end, Reporting Party(ies) (especially if anonymous) should diligently and regularly check the Whistleblowing Hotline using their own access codes to ensure that the Compliance Officer's requests are promptly reviewed and fulfilled. Lack of information or other evidence, including the Reporting Party's reluctance to cooperate with an investigation, may be the reason why the Compliance Officer decides to conclude that there is no concrete reason to proceed.

The investigation phase can be concluded with:

- negative outcome, in which case the Alert is dismissed;
- positive outcome: in this case, a written report summarizing the alleged facts, the investigations conducted and the factual findings as well as any recommendations elaborated by the Compliance Officer will be elaborated. Following review of this report, the Compliance Officer will elaborate, together with the Human Resources Function of the Company and with the other Functions interested by the Alert, a proposal re: any disciplinary, legal or administrative proceedings to be brought against the Reported Individual(s) and the other people targeted and submit it to the Company's BoD.

Within 3 months from the date of the Alert, feedback on the outcome of the investigation shall be provided to the Reporting Party. If, for objective reasons related to the complexity of the investigation, the investigation is not concluded within this period, the Compliance Officer will nevertheless provide the Reporting Party with feedback on the ongoing activities and initial outcomes of the investigation, reserving the right to provide further feedback when the activities are concluded. In any case, the content of such feedback should be made in such a way not to jeopardize any action taken by the Company as a result of the investigation and/or any ongoing investigations conducted by Public Authorities into the same facts.

Any potential disciplinary proceeding instituted against the Reported Individual and/or any other person identified as at fault following the internal investigation shall take place in accordance with applicable internal Company rules and the relevant labor regulation applicable.

On a semestral basis, the Compliance Officer provides to the Board of Directors of the Company a summary of reports received and for which an investigation has been opened, as well as a summary of reports received and found to be ungrounded, with an indication of the investigation conducted and the reasons why the

reports were found to be ungrounded.

7. Identity of the Reporting Party and Confidentiality Requirements

The Reporting Party is encouraged to identify himself or herself when reporting an Alert.

When the Reporting Party is not anonymous, his/her identity (and/or the information that could allow for his/her identification) is only known to the Compliance Officer and to the HR function to the extent this is necessary to protect the Reporting Party.

Thus, the identity of the Reporting Party will be treated confidentially and may not be communicated to anyone (including the Reported Individual) without the Reporting Party's prior approval, unless the dedicated recipients or other person involved in processing the Alert are required to report the facts to judicial authorities. In this case, the Reporting Party will be informed of the disclosure, unless this information is likely to compromise the legal proceedings.

In particular, as part of any disciplinary procedure initiated against a person mentioned in the Alert, the identity of the Reporting Party may be disclosed only if the Reporting Party explicitly consents.

Violation of the duty of confidentiality gives rise to disciplinary liability, without prejudice to other forms of liability provided by law.

The same confidentiality requirements also apply to the persons involved in the investigation or otherwise mentioned in the Alert.

When the Reporting Party is anonymous, the Alert will be processed if the gravity of the facts is established and the elements shared by the Reporting Party are sufficiently detailed, if necessary upon integration of the elements through the Whistleblowing Hotline following a specific request in this sense by the Compliance Officer.

8. Prohibition of Retaliatory and/or Discriminatory Acts

Bona fide Reporting Parties must be protected from any form of retaliation, discrimination or penalization, without prejudice to any other protection provided by law.

By way of example only, the following are considered forms of retaliation:

- dismissal, suspension or equivalent measures;
- downgrade or non-promotion;
- change of duties, change of work location, reduction of pay, change of working hours;

- suspension of training or any restriction of access to training;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- intimidation, harassment or ostracism;
- discrimination or otherwise unfavorable treatment;
- the failure to convert a fixed-term employment contract to a permanent employment contract when the employee had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including image damage, particularly on *social media*, or economic or financial damage, including loss of economic opportunities and income;
- improper listing on the basis of a formal or informal sector or industry agreement, which may result in the inability to find employment in the sector or industry in the future;
- early termination or cancellation of a contract for the provision of goods or services;
- the cancellation of a license or permit;
- the request to undergo psychiatric or medical examinations.

Reporting Parties who believe they have been subjected to retaliatory conduct as a result of a previously made Alert may notify ANAC of any form of retaliation they believe they have experienced (see section 9 below).

Acts done in violation of the above prohibition shall be null and void. Reporting Parties who have been fired as a result of an Alert have the right to be reinstated in their jobs and/or to obtain any protection guaranteed by applicable local law.

In addition to the protection afforded to the Reporting Party, the above protection measures will also be afforded to the following individuals/entities, referred to as "**Other Protected Persons**"

- (a) facilitators (i.e., those who assist the Reporting Party in the reporting process, operating in the same work context and whose assistance must be kept confidential);
- (b) persons who are in the same work environment as the Reporting Party and who are related to him or her by a stable emotional or family relationship within the fourth degree (e.g., relatives);
- (c) Reporting Party's colleagues who work in the same work environment as him/her and have a regular and current relationship with him/her;
- (d) entities owned by the Reporting Party, as well as entities operating in the same work environment as the Reporting Party;
- (e) other persons as specified in locally applicable laws.

9. External Reporting

In case the Reporting Party has:

- already made an internal report according to this Procedure that has not been acted upon within the

timeframe established in the same Paragraph; or

- reasonable grounds for believing that, if he/she made an internal report, it would not be effectively followed up or that the report itself might pose a risk of retaliation; or
- reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest;

the Reporting Party may make an external report ("**External Report**") to ANAC (National Anti-Corruption Authority). The Reporting Party making an External Report will be subject to the protection under this Procedure.

The report may be made in written or oral form through the channel implemented by ANAC and available at <https://whistleblowing.anticorruzione.it/#/>. ANAC must ensure strict confidentiality of the identity of the Reporting Party, the person(s) involved and the person(s) otherwise mentioned in the report, as well as of the content of the report and related documentation.

10. Processing of personal data

The Company adopts its model for the receipt and management of internal Alerts by identifying proper technical and organizational measures to ensure a level of security appropriate to the specific risks arising from the processing performed, on the basis of a data protection impact assessment, and by regulating the relationship with any external providers which process personal data on its behalf. Therefore, the Company has developed the necessary documentation for the express consent of the reporting person as provided for by Article 12 paragraph 2 of Legislative Decree No. 24/2023 and, during disciplinary proceedings, as provided for by Article 12 paragraph 5 of Legislative Decree No. 24/2023, as well as the documentation for the authorization of data processing to be submitted to the reporting persons, as identified by Article 12 paragraph 2 of Legislative Decree No. 24/2023, and identifies each data processing and each communication of personal data in accordance with Article 13 paragraph 1 of Legislative Decree No. 24/2023.

The processing of personal data received with the receipt and management of reports is carried out by the Company, as data controller, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU)2016/679 or Articles 3 and 16 of Legislative Decree No. 51/2018.

The Company provides appropriate information to the Reporting Party and the Referenced Individuals, pursuant to and for the purposes of Articles 13 and 14 of the same Regulation (EU) 2016/679, or Article 11 of the aforementioned Legislative Decree No. 51/2018, and adopts appropriate measures to protect the rights and freedoms of the persons concerned.

The privacy policy is available on the Whistleblowing Hotline.