







Reports of unlawful acts - "whistleblowing"
INFORMATION PURSUANT TO ART. 13 OF REGULATION (EU) 2016/679

	DATA CONTROLLER KIKO S.p.A., based in Bergamo via Giorgio e Guido Paglia n.1/D, cap. 24122 P.Iva 02817030162 – C.F. 12132110151 ("Data Controller").
	DATA PROTECTION OFFICER (DPO) Email address dpo.kiko@kikocosmetics.com
	PERSONAL DATA PROCESSED <ul style="list-style-type: none"> • First name and surname of the whistleblower together with other information that the whistleblower would like to release such as telephone number, email address, postal address, etc. • Any "special" personal data referred to in Art. 9 of the GDPR and/or judicial data referred to in Art. 10 of the GDPR communicated by the whistleblower and/or acquired as part of the investigations or communicated by the person (s) involved.

 PURPOSES OF THE PROCESSING	 LEGAL BASIS FOR THE PROCESSING	 DATA RETENTION PERIOD AND NATURE OF THE PROVISION OF THE DATA
<p>Personal data is collected and processed for purposes closely related and instrumental:</p> <p>1) to the verification of the validity of the reports received and for their management in relation to activities and/or conducts that differ from the procedures implemented by the Data Controller for such purposes, meaning the violation of the ethical principles of referred to by the current internal and external regulations and/or unlawful or fraudulent conduct relating to employees, members of corporate bodies, KIKO Group companies or third parties (customers, suppliers, consultants, or independent contractors), which may result, directly or indirectly, in economic, financial and/or reputational damage;</p> <p>2) the disclosure of the whistleblower's identity to persons other than those competent to receive and follow up on the report, in the cases provided for D. Lgs. 10th March 2023 n. 24.</p>	<p>Purpose 1): Fulfilment of a legal obligation for the Data Controller, who is required, by the D. Lgs. 10th March 2023 n. 24, to establish a channel for the reception and management of reports.</p> <p>Purpose 2): Ex. Art. 12 co.2 and 6 of D.Lgs. 10th March 2023 n.24 for the purposes of revealing the whistleblower's identity: consent of the data subject. This consent will be collected digitally or on paper by the Data Controller using a special form.</p>	<p>Data is processed in paper form or in electronic format in compliance with Art. 32 of GDPR 2016/679 on security measures. The reports received and the supporting documentation are kept, by the Data Controller's Global Audit department or by the subjects designated by it, at the Data Controller's premises, subject to the adoption of all appropriate precautions to guarantee maximum confidentiality.</p> <p>Without prejudice to specific provisions of the law, as well as the specific competences of the Supervisory Bodies of the Data Controller, as Collegio Sindacale and Organismo di Vigilanza, access to data relating to reports is allowed only to those authorised subjects.</p> <p>Personal data will be kept for a period of time not exceeding that necessary for the purposes for which they were collected and processed and, in any case, for no more than five years from the date of communication of the final outcome of the reporting procedure, except in the case in which a judicial and/or disciplinary action is initiated against the data subject or the whistleblower who has made bad-faith, false or defamatory statements; in such cases, personal data may be kept until the final conclusion of the judicial and/or disciplinary proceeding.</p> <p>Personal data processed for the purpose of revealing the whistleblower's identity to persons other than those</p>

		<p>competent to receive and follow up on the report are stored until the consent is revoked and unless the identity has already been revealed to third parties. Finally, personal data that is manifestly not useful for the processing of a specific report is not collected or, if accidentally collected, it is deleted immediately.</p>
<p>Once the storage periods indicated above have expired, the data will be destroyed, deleted, or made anonymous.</p>		



RECIPIENTS OR CATEGORIES OF RECIPIENTS OF PERSONAL DATA, PERSONS AUTHORISED TO PROCESS, AND DATA PROCESSORS

Internal access to personal data processed as part of the management of reports is allowed only to authorised personnel, identified by the Data Controller for the management of reports pursuant to the D. Lgs. 10th March 2023 n. 24.

Subsequently, where necessary for the management, assessment and investigation of the report, personal data may be communicated to individuals – appointed persons authorised to process personal data – the communication will only concern the data necessary for the performance of the tasks entrusted to the persons in charge, who will belong to the following categories: employees or seconded, temporary employees, interns belonging to the Global Audit department and to those other departments of the company necessary to conduct the investigation associated with the complaint received.

The data collected may be communicated to the subjects to whom this communication must be made in compliance with a legal obligation, a regulation or European legislation, if this is required (for example, for any subsequent criminal proceedings or if the whistleblower has made a false statement).

In compliance with D. Lgs. 10th March 2023 n. 24, in the event that, at the outcome of the investigations, the report is not manifestly unfounded, the Global Head of Audit – in relation to the profiles of illegality found and the contents of the report – identifies the subjects to whom to forward the report from among the following: (i) Organismo di Vigilanza, in cases where the report concerns breaches relevant pursuant to Legislative Decree No. 231 of 8 June 2001 and/or in any case, breaches of the Organisation, Management and Control Model adopted by the Company can be assumed (ii) the person in charge of the disciplinary proceedings against the accused for the sole purpose of initiating those proceedings (iii) the Data Protection Officer (DPO); (iv) the Judicial Authority, the Court of Auditors, ANAC or, where existing, additional Judicial Authorities or competent public bodies for their respective competence, where provided for by applicable law.

The Global Head of Audit may communicate the follow-up of the report to the Board of Director, for any further actions that may be necessary.

In the event of transmission of the report, the authorised department communicates only the contents of the report, eliminating any reference from which it is possible to trace, even indirectly, the identity of the whistleblower and of the other subjects whose identity must be protected.

As provided for art. 5 of D.Lgs. 10th March 2023 n.24, the Data Controller has activated an internal reporting channel that enables the reception and management of reports and which guarantees, also through the use of encryption tools, the confidentiality of the identity of the whistleblower, the person involved and the person possibly mentioned in the report. The service is provided by an external third-party company, *Whistleblowing Solutions Impresa AB*, with registered office in Norrgatan 10, 432 41 Varberg, Sweden, with which KIKO S.p.A., as Data Processor, has entered into a service contract, and which has been formally appointed Data Processor pursuant to Art. 28 of Regulation (EU) 2016/679.



TRANSFER OF PERSONAL DATA TO COUNTRIES OUTSIDE THE EUROPEAN UNION

There are no data transfers outside the European Union.
If for the Data Controller's specific needs, the data must be transferred to countries located outside the EU, the Data Controller promises to guarantee adequate levels of protection and safeguarding according to the applicable rules, including the provision of standard contractual clauses.



RIGHTS OF THE DATA SUBJECT

The GDPR recognises and guarantees specific rights (Articles 15 – 22 of EU Regulation 2016/679), including the right to know the data concerning the data subject (as a whistleblower, reported person, witness, etc.) held by the Data Controller for the whistleblowing reporting process, as well as how they are used and to obtain, when the conditions are met, the deletion, opposition, limitation, as well as the updating, rectification or, if there is an interest, the supplementing of the data.

The rights of the data subject (in particular, the reported party) may be limited pursuant to Art. 23 of EU Regulation 2016/679, if the exercise of the rights indicated above may result in an actual, effective impairment of the confidentiality of the whistleblower's identity.

The assessment of the need to limit the rights of the data subject is left to the Data Controller, who makes use of the relevant departments to do so.

In this case, the Data Controller must provide a reasoned communication without delay to the data subject of the rejection/delay/limitation/exclusion of the request to exercise the rights indicated above.

If access to a data subject's personal information is granted, the personal information of third parties such as whistleblowers, reported persons, or witnesses must be removed from the documents, other than in exceptional circumstances (if the whistleblowers authorise such a disclosure, if this is required by any subsequent criminal proceedings, or if the whistleblower has made an intentionally false statement).

METHODS OF EXERCISING THE RIGHTS

To exercise the rights described in the previous paragraph, the data subject may contact: dpo.kiko@kikocosmetics.com.

The deadline for the response is one (1) month, extendable by two (2) months in particularly complex cases; in these cases, the Data Controller will provide at least one interim communication within one (1) month of receiving the request.

COMPLAINT OR REPORT TO THE COMPETENT SUPERVISORY AUTHORITY

The Data Subject has the right to lodge a complaint or make a report or appeal to the Competent Supervisory Authority for the processing of personal data.

The Data Subject has the right to lodge a complaint or make a report to the Personal Data Protection Guarantor, or alternatively to appeal to the Judicial Authority. The Personal Data Protection Guarantor's contact details can be found on its website <http://www.garanteprivacy.it>.