

Information on the processing of personal data - Article 13 GDPR

Giorgio Armani S.p.A. ("**Company**", "**Armani**" or "**Data Controller**") informs you that Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/CE, the General Data Protection Regulation (hereinafter "**Regulation**"), provides for the protection of individuals with regard to the processing of personal data. This notice, pursuant to Article 13 of the Regulation and in accordance with the Whistleblowing Policy adopted by the Company (hereinafter "**Policy**"), contains the information regarding the processing of personal data contained within reports concerning violations of provisions of national or European Union Law which threaten the public interest or the Company's integrity, as well as violations of the principles and values provided by the Company's Code of Ethics and Policy, which the interested parties have become aware of in a work-related context, as governed by Italian Legislative Decree 24/2023 (hereinafter "**applicable legislation**").

Definition	Description
Anonymous report	An oral or written communication of information concerning a suspected or alleged violation within the meaning of the Policy, in which the Whistleblower's identity is unknown or untraceable
Concerned party/parties	Natural person/persons or legal entity/entities mentioned in the Whistleblowing Report as those whom the violation is attributed to and those with whom they are associated with
External company	The External consulting Company formally appointed by the Armani Group to manage its internal Reporting channel and the preliminary assessment of Whistleblowing reports
Facilitator	A natural person who assists a Whistleblower in the reporting process, operating in the same Work-related context and whose assistance should be confidential
Legislative Decree 231/2001	Legislative Decree No. 231 of 8 June 2001, concerning the administrative liability of companies and legal entities
Privacy Code	Legislative Decree no. 196 of 30 June 2003
Supervisory Body	The Supervisory Body withing the Armani Group's Italian Companies which have adopted a 231 Model
Whistleblower or Whistleblowers	A natural person who reports information on violations within the meaning of the Policy, acquired in the context of their work-related activities
Whistleblowing Channel	The Internal Whistleblowing Channel adopted in accordance with the Policy
Whistleblowing Report	An oral or written communication of information concerning a suspected or alleged violation within the meaning of the Policy
Work-related context	Current and past work or professional activities through which, regardless of the nature of those activities, persons acquire information on violations and within which they may suffer Retaliatory measures as a consequence of a Report, Public disclosure or complaint to the authorities
231 Model	Organisation and management model pursuant to Legislative Decree 231/2001, with reference to Article 6 of Legislative Decree 231/2001

1. Processed data

The Company collects, processes, and uses the following types of personal data (collectively, "**Personal Data**"):

- Personal details, such as the Whistleblower's name and surname, and/or, if provided, the names and surnames of any other Concerned parties or other persons mentioned in the Whistleblowing Report;

- Contact details, such as the Whistleblower’s email address and phone number, and/or, if provided, the email address and phone number of any other Concerned parties or other persons mentioned in the Whistleblowing Report;
- In cases where the Whistleblower is an employee, a collaborator, a trainee, an employee during his/her trial period, a Facilitator or a person involved in an administrative, management, supervisory or representative role, even information regarding their employment, such as their current position;
- Information which may have been collected during the preliminary assessment, during the assessment of the Whistleblowing report’s admissibility and, where applicable, during investigation activities.

In addition, we collect, process and use special categories of personal data as per Article 9 of the Regulation, which may be found within the Whistleblowing Report and in its attached documentation referring to or provided by the Whistleblower, or even collected after verifying whether the Whistleblowing Report is sufficiently founded, in accordance with the Policy (collectively, "**Special - Sensitive Data**").

Finally, we collect, process and use the data as per article 10 of the Regulation which may be contained in the Whistleblowing Report referring to or provided by the Whistleblower, or even collected after verifying whether the Whistleblowing Report is sufficiently founded, in accordance with the Policy (collectively, "**Judicial Data**").

In accordance with the provisions of the applicable legislation and the Policy, Anonymous reports shall always be permitted. The processing of Personal Data and any Sensitive Data and Judicial Data which may be contained within the Whistleblowing Report will be carried in compliance with the applicable legislation and the Policy’s contents. Personal Data and any Sensitive Data and Judicial Data which may be contained within the Whistleblowing Report will be collected only where a Whistleblowing Report has been made, with no Personal Data collection occurring in cases of Anonymous reports.

2. Processing operations

Data processing takes place through the collection, recording, organisation, storage, consultation, elaboration, modification, selection, extraction, comparison, use, combination, restriction, dissemination, erasure, and destruction of the provided data for the purposes set out under paragraph 4 below.

With reference to Personal Data or any Sensitive or Judicial Data, if provided in the Whistleblowing Report, the Company shall apply:

- Encryption techniques, in order to guarantee their privacy and confidentiality, as well as the privacy of the Whistleblower;
- Anonymisation techniques, in accordance with the retention period, referred to in paragraph 9 below;
- Irreversible anonymisation techniques/erasure upon expiration of the retention period, referred to in paragraph 9 below.

3. Purpose of and legal basis for processing

Personal Data and any Sensitive or Judicial Data provided in the Whistleblowing Report are collected, processed and used for the purposes outlined below:

Purposes of processing	Legal basis
-------------------------------	--------------------

-
- 1. **To manage the illicit conduct reporting system** aimed at:
 - i. preventing and effectively combating fraudulent and unlawful or irregular conduct within the Company’s internal organisation system, in particular for the fulfilment of the obligations as provided by the applicable legislation and Article 6 comma 2-bis of Legislative Decree 231/01, introduced by Law 179/2017, which may involve the processing of the Whistleblower’s personal details and of Concerned party in order to implement adequate internal Whistleblowing Channels
 - ii. preventing, managing and carrying out the assessment of the potential illicit conducts or behaviour that have been reported;
 - 2. To comply with requests made by the competent administrative or judicial authorities and, more generally, from public entities in compliance with the legal formalities.
-
- 3. **To adequately manage internal corporate governance** through the Whistleblowing reporting system, by allowing You to make a Whistleblowing Report or an Anonymous report, and by allowing the Company to manage these in accordance with the Policy, with assessment and supervisory activities aimed at combating crime;
 - 4. **To prevent and suppress unlawful acts, even on disciplinary grounds**, as well as to protect the rights and interests of the Data Controller and/or of third parties, even in judicial proceedings.
-
- 5. **To disclose the Whistleblower’s identity.** The Whistleblower’s Personal Data, prior the latter’s consent, may be disclosed when the Whistleblowing Report is used during disciplinary and/or judicial procedures which may have commenced, in such cases where the dispute is based on the Whistleblowing Report, whether wholly or partially, and the disclosure of the Whistleblower’s identity is essential to the Concerned party’s defence in the context of said procedures. In such cases, free, specific and expressed consent shall be granted by the Whistleblower only if the above necessities should arise, with prior notice being provided to the Whistleblower via a written communication of the reasons for the disclosure of their Personal Data.
-
- (i) The fulfilment of legal obligations to which the Company is subject to (Article 6, paragraph 1, letter c) GDPR regarding Personal Data and articles 9.2 letter c) and 10 GDPR with regard to any Sensitive and Judicial Data provided).
 - (ii) Legitimate interest of the Company or a third party.
 - (i) Whistleblower’s consent, pursuant to Article 6.1, letter a) of the GDPR.
-

4. Consequences of non-disclosure of data

The provision of Personal, Sensitive or Judicial Data for the purposes outlined above is voluntary and optional, and, if not granted, no consequences shall incur other than the impossibility of following up on Whistleblowing Reports. In any case, unless the Personal, Sensitive and Judicial Data have been provided to the Company, Anonymous reports shall always be permitted as further described in paragraph 2 of this document.

5. Right of access

Access to Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report may be granted to:

- Personnel within the Company authorised to manage the Whistleblowing Report and the Anonymous Report, duly instructed and appointed on contract;
- The Supervisory Body, where necessary (that is, if the Whistleblowing Report were to concern violations of the 231 Model adopted by the Company);
- External persons appointed as Data Processors in accordance with Article 28 of the Regulation (i.e. the External Company), specifically identified by the Data Controller, duly instructed on processing methods and purposes and bound by the appropriate privacy and confidentiality obligations.

Any access to Personal Data and to any Sensitive and Judicial Data provided in the Whistleblowing Report is limited to the persons who need to be aware of these in order to fulfil their responsibilities in relation to the management of the Whistleblowing Report.

6. Data disclosure

With exception of the cases outlined in paragraph 4 of this document, Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report may be disclosed to third parties in the following cases:

- When disclosure is required by applicable laws and regulations with respect to legitimate third-party recipients, which may be competent authorities and public entities such as supervisory/inspection bodies, law enforcement and the judiciary, which process the data in the capacity of autonomous data controllers for their own respective institutional purposes or as provided by the law, e.g. in the context of a legal dispute;
- To consultants or lawyers, even associated in a firm, who provide legal counsel to the Company and who process the data, depending on the case, as either autonomous data controllers or as data processors pursuant to Article 28 of the Regulation, in order for the Company to exercise its right to defend itself in the context of legal disputes which may derive from the Whistleblowing Report, as granted by Article 24 of the Constitution;
- To subsidiary or affiliate companies pursuant to Article 2359 of the Civil Code, to the extent of their competencies (for example, if the Whistleblowing Report or Anonymous report were to also concern their employees).

The Company guarantees the utmost care to ensure that disclosure of the Personal Data and of any Sensitive and Judicial Data provided in the Whistleblowing Report to the above recipients involves solely Personal data which are strictly necessary to achieve their specific intended purpose.

Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report will not be in any way subject to dissemination.

7. The transfer of data outside of the EU

Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report will not be transferred to countries outside the European Union.

8. Retention period

Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report are stored by the Company strictly to the extent necessary for the fulfilment of our obligations and strictly for the time necessary to achieve the purpose for which the information has been collected, in compliance with the applicable legislation on the protection of personal data. When we will no longer have use for Your Personal, Sensitive and Judicial Data, we shall erase these from our systems and archives and/or we will implement provisions to permanently anonymise them, so that You may no longer be identified through these (unless we were obliged to retain Your information to fulfil the legal or regulatory requirements the Company is subject to). Personal Data and any Sensitive and Judicial Data provided in the Whistleblowing Report are subject to a 5-year retention period, as provided by the applicable legislation, which shall commence on the date the final feedback of the Whistleblowing Report's process is communicated.

If a legal dispute concerning the assessment of the facts reported in the Whistleblowing Report should arise following the final feedback of the Whistleblowing Report's process, we may retain the Personal Data, as well as any Sensitive and Judicial Data provided in the Whistleblowing report, for up to 10 years commencing on the date the judicial ruling is final.

9. Your rights

You may at any time contact the Company, acting as the Data Controller or the Data Protection Officer, via the contact details provided in the following paragraph, to obtain an up-to-date list, which is kept by the Data Controller, of our data processors (namely our service providers) and of persons whom the data is disclosed to, and to exercise at any time the following rights as outlined in Articles 15 ff. of the Regulation.

You may at any time withdraw the consent you may have given for processing your data with future effect. Such a withdrawal will not prejudice the lawfulness of any processing prior to the consent withdrawal. As provided by the Regulation, You have the right to file a complaint to the competent national supervisory authority and to contact the supervisory authority in case of any restrictions in exercising your rights. In accordance with the Regulation, aside from any limitations provided by the law (for example, limitations provided for in Article 2-undecies of the Privacy Code), you have the right to:

- Request access to Your personal data: You may have the right to obtain from us confirmation as to whether or not personal data concerning You is being processed, and in such case, to request access to the personal data. The accessible information includes, among other, the purposes of the processing, the categories of personal data concerned and the recipients or categories of recipients to whom the personal data have been or will be disclosed. However, this is not an absolute right, and the interests of other persons may limit your right of access. You may have the right to obtain a copy of the personal data being processed. For additional copies you may request, we could charge a reasonable fee based on administrative costs.
- Request the rectification of Your personal data: You may have the right to obtain from us the rectification of inaccurate personal data which concern you. Taking into account the purposes of the processing, you may have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- Request the erasure of Your personal data: in certain circumstances, You may have the right to obtain from us the erasure of personal data concerning You and we may have the obligation to erase such personal data.
- Request the restriction of Your personal data: in certain circumstances, You may have the right to obtain from us the restriction of processing Your personal data. In this case, the respective data will be flagged and may be processed by us only for certain purposes.

- Request data portability: in certain circumstances, You may have the right to receive the personal data concerning You, which you have provided us with, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another entity without hindrance from us.
- Object to the processing of Your personal data: in certain circumstances, You may have the right to object, on grounds relating to his or her particular situation, at any time to our processing of Your personal data and You may ask us to no longer process Your personal data.

10. The Data Controller and the Data Protection Officer

The Data Controller is Giorgio Armani S.p.A. – registered office at Milano, via Borgonuovo, 11 - 20121 (MI) - email: privacy@giorgioarmani.it. The Data Protection Officer, the head of the Data Protection department, Rödl & Partner, Largo Donegani 2, Milano, is reachable via the following email address: dpo@giorgioarmani.it.

Should you have any question regarding this notice, you may contact the Data Controller or the Data Protection Officer at any time. The Company may update this notice from time to time in accordance with the applicable legislation (for example, in case a new reporting system were to be adopted), and in such case we will duly inform you about any such amendments.