

INFORMATION ON THE PROCESSING OF THE REPORTED PERSON'S PERSONAL DATA

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 ('GDPR')

Pursuant to the Regulation (EU) 2016/679 ("GDPR"), Salvatore Ferragamo S.p.A. ("**Ferragamo**", "**Company**" or the "**Data Controller**") provides this notice regarding the processing of your personal data in the context of the management of the reporting process of unlawful conducts ("**Whistleblowing**"), in which you are involved as a reported subject or as a third party (so called Whistleblowing).

Whistleblowing report means any communication received by Salvatore Ferragamo S.p.A. concerning conduct attributable to Salvatore Ferragamo S.p.A.'s employees in breach of the Code of Ethics, laws, regulations, provisions of the Authorities, internal rules, the Organizational, Management and Control Model pursuant to Legislative Decree 231/2001 ("Model 231") or Compliance Models for the Company's subsidiaries, in any case capable of causing damage or harm, even if only in terms of image, to Salvatore Ferragamo S.p.A.

If you have any questions regarding this policy and/or the processing of your personal data, you may contact the Data Controller and/or the Data Protection Officer at any time at the contact details indicated below.

1. Identity and contact details of the data controller

The Data Controller is **Salvatore Ferragamo S.p.A.**, with registered office in Via dei Tornabuoni, no. 2 - 50123 - Florence, VAT no. 02175200480.

2. Contact details of the Data Protection Officer (DPO)

The Controller has appointed a Data Protection Officer, who can be contacted at the following e-mail address: privacy@ferragamo.com.

3. Purpose of processing and legal basis for processing

The Controller will process your personal data relating to:

- any information provided in the Whistleblowing Report by the whistleblower;
- any information acquired in the course of the necessary investigative activities (e.g. public sources, third parties interviewed, etc.);
- information that you may have provided during the Whistleblowing Report handling process.

for:

- a) Purposes of compliance with regulatory obligations, legal obligations and provisions of Authorities empowered by law (Art. 6(1)(c) GDPR).

The Data Controller shall process the data for the purpose of preventing and effectively combating fraudulent and unlawful or irregular conduct and to support the effective application and operation of the 231 Model, as well as to manage and organise the Whistleblowing Reports received, also in accordance with the provisions of the Group Whistleblowing Policy, including activities of internal investigation and verification of the conduct subject to Whistleblowing Reports and the institution of proceedings, including disciplinary proceedings, within the limits of what is required by the applicable rules. In addition, personal data may be processed in order to comply with requests by the competent administrative or judicial authorities and, more generally, by public bodies in compliance with legal formalities.

For the purposes described above, personal data will possibly be processed for the fulfilment of legal obligations to which the Data Controller is subject. The provision of personal data is not mandatory, as permitted by law (e.g. in the case of anonymous reporting. In the latter case, the Company will assign you an identification code that will allow you, if you so

wish, to access the platform set up for Whistleblowing Reports by the Company, should you decide to use this means of reporting).

b) Further processing based on the legitimate interest of the Controller or a third party.

The Controller will also process personal data for:

- owner's internal control and business risk monitoring needs, as well as for the optimisation and streamlining of internal business and administrative processes;
- ascertain, exercise or defend a right or a legitimate interest of the data controller.

The legal basis for the processing is represented by the pursuit of the legitimate interest of the Data Controller (Art. 6(1)(f) of the GDPR) or of third parties, represented by the right of defence and the interest in guaranteeing the effectiveness and efficiency of the company's internal control and risk management system also in order to effectively prevent and counter fraudulent and illegal or irregular conduct. This legitimate interest has been duly assessed by the Controller.

4. Treatment modalities

The data - where provided and collected - will also be processed by electronic means, recorded in special digital archives, and used strictly and exclusively for the purposes indicated. Where appropriate in relation to the purposes illustrated, processing will be carried out in aggregate/anonymous form.

5. Authorised for processing

The Data will be processed by the members of the Ethics Committee as well as by the Company's staff acting on the basis of specific instructions as to the purposes and methods of processing and who will in any case only be involved in strictly necessary cases, taking care to preserve the absolute confidentiality of the data subjects.

Should the Whistleblowing Report or the information received by the Ethics Committee turn out to be related to violations inherent to offences pursuant to Legislative Decree No. 231/2001 or to violations of the Company's Organisational Model, the Data shall also be processed by the members of the Supervisory Board, which shall take decisions on the management thereof.

6. Recipients of personal data

For the pursuit of the purposes set out in point 3, your personal data may be disclosed to the Data Controller, to the persons authorised by the Data Controller to process the Whistleblowing Notice, and to the persons appointed as Data Processors pursuant to Article 28 of the GDPR. The latter will be specifically identified by the Data Controller, who will also provide specific instructions on the methods and purposes of the processing and ensure that they are subject to adequate obligations of confidentiality and privacy.

The Data Controller may also communicate, provided that this is necessary for the pursuit of the purposes of the processing and on the basis of the same conditions of lawfulness indicated in point 3, the personal data collected to third parties belonging to the following categories:

- **police forces**, competent authorities and other public administrations. These subjects will act as autonomous data controllers;
- **companies, bodies or associations**, i.e. parent companies, subsidiaries or associated companies within the meaning of Article 2359 of the Civil Code, or between these and companies subject to joint control, as well as between consortia, networks of companies and temporary groupings and associations of companies and their members, limited to the aspects falling within their competence (e.g. where the Report also concerns their employees). Unless otherwise indicated, these subjects will act as autonomous data controllers;
- **auditing/auditing companies and other companies contractually linked to the Data Controller** (also belonging to the same group) that perform, by way of example, consultancy activities, support for the provision of services, etc., which will act, as the case may be, as autonomous data controllers, or as data processors on the basis of a specific agreement on the processing of personal data concluded pursuant to Article 28 GDPR;
- **collegial bodies of the Company in charge** and only those persons strictly necessary to follow up the Whistleblowing Report who have committed themselves to confidentiality, including the facilitator, if any;

- **platform providers and companies providing management and maintenance services for** the information systems underlying the provision of the service with whom the Company has entered into contracts for the processing of personal data and who act as data controllers.

In particular, the Service is operated on behalf of the Company, by Integrity Line GmbH, with whom the Company has entered into a personal data processing agreement ("DPA") and who acts as a Data Processor within the meaning of Article 28 of the GDPR.

The Data Controller takes the utmost care to ensure that the communication of your personal data to the aforementioned recipients only concerns the data necessary to achieve the specific purposes for which they are intended. Your personal data will not be disseminated.

7. Transfer of personal data outside the European Economic Area

The data provided in connection with the Service may be transferred to Switzerland, the headquarters of the company Integrity Line GmbH, which operates the Service. The transfer is legitimised by the adequacy decision issued by the European Commission. This adequacy decision ensures that the applicable Swiss data protection regulations guarantee an adequate level of security and data protection measures similar to the European legislation, i.e. the GDPR.

The management of the database and the processing of such data are bound to the purposes for which they were collected and are carried out in strict compliance with the standards of confidentiality and security set out in the applicable data protection laws. Whenever your personal data should be transferred outside the European Economic Area and, in particular, to States that do not benefit from an adequacy decision of the European Commission, the Data Controller shall subscribe to the standard contractual clauses adopted by the European Commission and shall adopt any further technical and organisational measure suitable and necessary to guarantee an adequate level of protection of your personal data and in any event, at least equal to that guaranteed within the European Economic Area, in accordance with the provisions of this Privacy Policy, including, among others, the Standard Contractual Clauses approved by the European Commission.

8. Data retention period

The data will be stored in a dedicated digital archive and protected by appropriate security measures for a period of time not exceeding the time necessary to achieve the purposes for which they are collected and for any longer period necessary to comply with legal provisions and/or for the purposes of judicial protection, in compliance with ordinary prescriptive periods.

In detail, in accordance with the Group Whistleblowing Policy, Whistleblowing Reports and related documentation are kept by the Ethics Committee:

- for 1 (year), if dismissed as unfounded;
- for as long as is necessary for the processing of the Whistleblowing Report and in any case no longer than 5 (five) years from the date of communication of the final outcome of the Whistleblowing procedure, in compliance with the confidentiality obligations enshrined in the Whistleblowing Decree, Foreign Whistleblowing Laws, the Privacy Code, the GDPR and/or other applicable data protection laws. After 5 years, Whistleblowing Reports and related documentation will be deleted.

Data that are manifestly not useful for the processing of a specific Whistleblowing Report are not collected or, if accidentally collected, are deleted immediately.

At the end of the storage period, your personal data will be deleted or irreversibly anonymised.

9. Rights of data subjects

As a data subject, you are granted, where applicable and within the limits identified by the relevant legal provisions, the rights summarised below.

Right of Access

You have the right to obtain confirmation from the controller as to whether or not personal data concerning you are being processed and, if so, to obtain access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data in question;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular if they are recipients in third countries or international organisations;
- where possible, the intended period of retention of personal data or, if this is not possible, the criteria used to determine that period;
- the right to lodge a complaint with a supervisory authority;
- if the data are not collected from you, all available information on their origin.

It is understood that your confidentiality will be protected to the fullest extent permitted, with particular reference to your identity, which will not be disclosed to the reported person or to third parties, except where necessary for the purposes of judicial protection, to comply with legal obligations, and always within the limits provided for by law, in order to avoid retaliation, threats, violence, discrimination, etc., direct or indirect against you for reasons directly or indirectly related to the Whistleblowing Report. The confidentiality of your identity shall not be guaranteed in the event of an unlawful Whistleblowing Report (i.e. a report which, on the basis of the results of the preliminary investigation phase, is found to be unfounded on the basis of objective elements, and in respect of which the concrete circumstances ascertained during the same preliminary investigation allow for the belief that it was made in bad faith or with serious negligence).

Right of rectification and cancellation

In the cases provided for by the applicable legal provisions, you may exercise the right to obtain the rectification of inaccurate personal data concerning you without undue delay as well as, taking into account the purposes of the processing, the right to obtain the integration of incomplete personal data, including by providing a supplementary declaration.

You also have the right to obtain the deletion of personal data concerning you if one of the following reasons applies:

- personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- data are unlawfully processed;
- objected to the processing activity and there is no overriding legitimate reason;
- personal data must be deleted to fulfil a legal obligation.

However, the Data Controller has the right to reject the request for deletion if the right to freedom of expression and information prevails or for the exercise of a legal obligation, to defend its own right in court or for the legitimate interest of the Data Controller.

Right to restriction of processing

You have the right to obtain from the Company the restriction of processing in the following cases:

- for the period necessary for the Controller to verify the accuracy of the data contested by the data subject;
- in case of unlawful processing of personal data;
- even if your personal data are not necessary for the purposes of processing, you need them for the establishment, exercise or defence of a legal claim;
- for the period necessary to verify whether the Controller's legitimate reasons prevail over your request to object to the processing.

Right of opposition

You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you on the basis of legitimate interest within the meaning of Article 6(1)(f) GDPR. This is without prejudice to the possibility for the Controller to continue the processing by demonstrating the existence of compelling legitimate grounds that override your interests, rights and freedoms.

Right to lodge a complaint and/or appeal

You have the right to lodge a complaint with the Data Protection Authority and/or appeal to the courts.

The Data Controller reserves the right to limit or delay the exercise of these rights, within the limits set by the applicable provisions of law, in particular where there is a risk of actual, concrete and not otherwise justified prejudice to the confidentiality of the identity of the Whistleblower and where the ability to effectively verify the merits of the Report or to gather the necessary evidence may be compromised (see Articles 2-undecies and 2-duodecies of the Privacy Code and Article 23 of the GDPR).

The exercise of such rights shall also be carried out in accordance with the provisions of the law or regulations governing the sector (including Legislative Decree No. 231/2001 as amended by Law No. 179/2017, as well as EU Directive No. 2019/1937 as implemented by Legislative Decree No. 24/2023).

Please note that pursuant to Article 2 undecies of Legislative Decree 196/2003 (as amended and supplemented), the rights set out in Articles 15 to 22 of the Regulation may not be exercised by making a request to the Data Controller or by lodging a complaint pursuant to Article 77 of the Regulation if the exercise of such rights would cause actual and concrete prejudice to the confidentiality of the identity of the person making a Whistleblowing Report, which prejudice will be assessed on a case-by-case basis, in concrete terms, and only where it is a necessary and proportionate measure. Where the Company makes use of this limitation, it will be notified without delay, in writing.

If you have provided a Whistleblowing Report through the oral channel, you may revoke your consent to the recording of the call.

The response time stipulated by European legislation to which we are subject is one month from your request (extendable up to a further two months in cases of particular complexity).

Finally, we remind you that you may lodge a complaint with the supervisory authority of your Member State of residence, if you are a resident of the European Union. In any event, you have the right to lodge a complaint with the Italian supervisory authority (<http://garanteprivacy.it/>) if you consider that the processing of your personal data is contrary to the legislation in force.

You may exercise the rights listed above by writing to the Data Controller at the contact details given in section 1 or by writing to the Data Protection Officer at privacy@ferragamo.com.

This notice is updated on 26/07/2023.