

# Speak Up Privacy Policy

OCT 2024

## Speak Up Privacy Policy

**Last Updated: 1<sup>st</sup> October, 2024**

L'OCCITANE International (Suisse) SA, which is headquartered in Switzerland, ("**LOI**"), its affiliates and its brands ("**Affiliate**") (together the "**L'OCCITANE Group**") have implemented a Speak Up procedure to report possible violations of the L'OCCITANE Group Code of Business Conduct and/or a law/regulation.

**The Speak Up reporting procedure:** the [L'OCCITANE Group Speak Up Policy](#) describes the conditions for implementing the Speak Up reporting procedure.

You can choose to report internally through either of the two following channels:

- The Local Speak Up channel available in your country, with the contact person designated by the local Affiliate.
- The Group Speak Up channel, set up by LOI.

If you submit a Speak Up report ("**Report**") and give your contact information, you will receive a confirmation of receipt within seven days, or within the period specified by local law, if it imposes more restrictive delays.

Please refer to the [Group Speak Up Policy](#), which contains essential information regarding the implementation of the reporting procedure and should be read in conjunction with this Speak Up Privacy Policy (the "**Policy**").

**This Policy:** This Policy relates to the collection and processing of personal data ("**Personal Data**") in the context of a Report. When Reports are made, LOI or the local Affiliate will process personal data in order to:

- Process Reports received.
- Investigate Reports and carry out the necessary checks and analyses.
- Determine the actions to be taken on Reports.
- Protect individuals.
- Exercise or defend legal rights.

This Policy explains how LOI and/or its Affiliates collect and process your Personal Data in the context of the reporting system and the subsequent investigation of the reports. This Policy also tells you about your rights with respect to your Personal Data.

To the extent that local law imposes higher standards than those set out in the present Speak Up Privacy Policy, the local law will apply.

**Abusive use of the Speak Up channel may expose their authors to sanctions and legal proceedings. However, using the Speak Up channel in good faith will not result in any disciplinary sanction, even if the facts reported are incorrect or do not lead to any formal action being taken.**

## I. Relevant Data Controllers

- **Reports submitted through the Local Speak Up channel:** When a Report is submitted through the Local Speak Up channel, the local Affiliate acts as the data controller.
- **Reports submitted through the Group Speak Up channel:** When a Report is submitted through the Group Speak Up channel, LOI acts as the data controller.

(Individually, the "**Data Controller**", "**we**" or "**our**").

The Data Controller processes Personal Data for the purpose of collecting and investigating Report based on the following legal grounds:

- **Legal obligation:** We have a legal obligation to use your Personal Data to comply with the requirements related to the implementation of reporting procedures; and
- **Legitimate interest:** We may have a legitimate interest in using your Personal Data, in particular to ensure compliance with the [L'OCCITANE Group Code of Business Conduct](#) and applicable laws and regulations. The Data Controller can only rely on its legitimate interest as a legal ground for the processing where this interest is not overridden by individuals' interests and fundamental rights and freedoms.

## 2. Individuals who can use the Speak Up Channel

The following individuals can use the Speak Up channel:

- Employees, interns and contractors of the L'OCCITANE Group
- Suppliers in the value chain and their employees
- Customers and prospects
- Community members

### 3. Personal Data We Collect

The Data Controller collects and stores data that relate to information that is relevant and necessary to the processing of the Report.

Data provided as part of Reports should be factual and directly related to the potential violation reported. Reports should not include data covered by national defense secrecy, medical secrecy, secrecy of judicial deliberations, secrecy of judicial inquiries or investigations, or the professional secrecy of lawyers.

When a Report is sent to the Data Controller, we may collect the following Personal Data:

- Facts reported.
- Identity, functions and contact details of:
  - Persons making Reports.
  - Persons mentioned in Reports.
  - Persons involved, consulted or heard in the processing of the Report.
  - Facilitators and persons in contact with person who has made the Report.
- Information gathered in the course of verifying the facts reported.
- Verification reports.
- Follow-up actions taken.

**Special categories of Personal Data:** Special categories of Personal Data (in particular Personal Data relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, health, trade-union membership, sexual life or sexual orientation) may be processed as part of the reporting process insofar as such process fulfills a substantial public interest or is necessary, where applicable, for the establishment, exercise or defense of legal claims.

**Personal Data relating to criminal convictions and offences:** Personal Data relating to criminal convictions or offences may be processed as part of the processing of a Report where such processing is necessary for the preparation and, where applicable, the exercise and follow-up of legal proceedings as victim, defendant or on their behalf, or as provided for by specific provisions of the applicable laws.

**Cookies:** Cookies may be used as part of the processing of Reports submitted through the Group Speak Up Channel or through the Local Speak Up Channel. For further information on the use of cookies, please refer to the Cookie Policy of our Speak Up service provider, which is available [here](#), or through the Local Speak Up Channel.

After a decision has been taken about the handling of the Report, we will only process Personal Data necessary in order to:

- Protect the stakeholders against the risk of retaliation.
- Exercise and defend legal rights.
- Carry out audits of our internal processes.

#### 4. Recipients of the Personal Data

The Personal Data referred to above may be disclosed to:

- Our Speak Up service provider(s) in charge of collecting Reports.
- External legal advisors and counsels assisting the Data Controller.
- For reports raised via the Global Speak Up Channel: the Group Internal Audit Department and/or with other internal stakeholders, depending on the nature of the investigation and the expertise required.
- For reports raised via the Local Speak Up Channel: the Human Relations Director and/or the General Manager and/or with other internal stakeholders, depending on the nature of the investigation and the expertise required.

The information related to the Report can only be shared for the purposes of verifying or processing the Report. Only information that is strictly necessary and proportionate to the purpose of the communication will be forwarded to the above-mentioned recipients.

The recipients of the information relating to the Report are bound by the same or equivalent strengthened contractual confidentiality obligation as the Group Internal Audit Department.

Information identifying the reporting person may only be disclosed with their consent, except to judicial authorities. In this case, the reporting person will be informed of the disclosure to the judicial authority, unless such information could compromise the proceedings.

Information that could identify the person implicated or any third party mentioned in the Report may only be disclosed, except to the judicial authority, once it has been established that the Report is well-founded.

## **5. Data transfers**

As part of the Speak Up reporting procedure and if permitted by law, the Personal Data of the persons concerned may be transferred to LOI located in Switzerland and/or to one or more local Affiliates located inside and outside the European Union, for the sole purpose of processing the Report. Please refer to the [latest annual report](#) for the localization of Affiliates.

We comply with applicable legal requirements when transferring Personal Data to countries other than the country where you are located. For instance, we may transfer your Personal Data to countries for which adequacy decisions have been issued or use contractual protections for the transfer of Personal Data. If you are located in the European Union, you may contact us as specified below to obtain a copy of the safeguards we use to transfer Personal Data outside of the European Union.

## **6. Retention period**

The Data Controller will retain data relating to a Report in its active databases until a decision is made about the processing of the Report.

Once the final decision on further action has been taken, the data may be kept in the form of intermediate archives, for a period of time that is strictly proportionate to processing of such data and to the protection of the individuals who have made the Report and the persons mentioned in the Report, taking into account the time required for any further investigations.

When disciplinary or litigation proceedings are launched against an individual or author of an abusive Report, the data relating to the Report may be kept by the Data Controller until the end of the procedure or of the period of limitations for an appeal against the decision.

Data may be kept for longer periods, in the form of intermediate archives, if the Data Controller is legally obliged to do so (for example, to meet accounting, social or tax obligations), or for evidential purposes in the event of an audit or dispute, or for the purposes of carrying out quality audits of the Report procedure.

We may keep anonymous or anonymized data indefinitely.

## 7. Informing the Subject of the Report

The Data Controller must ensure compliance with the principles of transparency and fairness with regard to persons whose data may be processed.

The Data Controller will inform the person concerned by a Report within one month of the Report being received. However, when precautionary measures are necessary, in particular to prevent the destruction of evidence relating to the Report or to preserve the confidentiality of the investigation, this person may be informed only after these precautionary measures have been taken.

The person concerned by a Report may under no circumstances obtain from the Data Controller, on the basis of his or her right of access, information concerning the identity of the reporting person, or of any third party mentioned in the Report.

## 8. Rights of data subjects

You may have certain rights in relation to your Personal Data. If you are in the European Union, these rights include the ones listed below. The rights of non-EU residents may differ in accordance with the local law.

- **Right of access:** Any person whose Personal Data is being or has been processed as part of the reporting procedure has the right of access to that personal data, in accordance with the GDPR.
- **Rights of rectification and erasure:** Persons identified in the reporting procedure have the right to request the rectification or erasure of their Personal Data if it is inaccurate, incomplete, equivocal or outdated. However, exercising this right will not retroactively modify the elements contained in the Report or collected during the investigation.

The aforementioned rights may not be used by the person who is the subject of a Report to obtain information relating to the identity of the reporting person.

- **Right to restrict the processing:** The right to limit processing may be exercised, for example, when the individual disputes the accuracy of their data, and may request a temporary freeze on processing while the necessary checks are carried out.

- **Right to object:** Pursuant to Article 21 of the GDPR, the right to object may not be exercised for processing necessary to comply with a legal obligation to which the Data Controller would be subject. For processing based on the legitimate interest of the Data Controller, the right to object may be exercised provided that the data subject provides reasons relating to his or her particular situation. This right of objection will not apply, however, if there are legitimate and compelling grounds which override the interests and rights of the data subject, or if the processing is necessary for the establishment, exercise or defense of legal claims.

## 9. Our Contact Information

If you have any questions or comments about this Policy, our privacy practices, or if you would like to exercise your rights with respect to your Personal Data, please contact us as follows:

- **If the Report is submitted through the Local Speak Up channel:** Contact the local Affiliate and/or refer to the Human Resource Department.
- **If the Report is submitted through the Group Speak Up channel:**
  - In writing by registered letter addressed to: L'OCCITANE International (Suisse) SA, Chemin du Pré Fleuri 5, 1228 Plan-les-Ouates, Suisse
  - By e-mail to the following address: [speakup@loccitane.com](mailto:speakup@loccitane.com)
  - Our Data Protection Officer can be contacted at the following address: [dpo@loccitane.com](mailto:dpo@loccitane.com)

The subject line of any paper or electronic mail should read "Strictly Confidential – Speak Up Report".

We will respond to such requests in accordance with applicable data protection legislation. If you believe that your Personal Data has been processed in violation of applicable law, you have the right to lodge a complaint with your local supervisory authority. If you are in the European Union your supervisory authority is the one in which you have your habitual residence or place of work, or place of the alleged infringement of applicable rules.

## 10. Changes to this Policy

We may update this Policy from time to time to reflect changes in our privacy practices or when required by data protection laws. We will bring any material changes to this Policy to your attention in an appropriate manner.