



PUIG

Reporting Channel Policy and Procedure



Reporting Channel Policy	4
Context for the reporting channel	5
Purpose and scope of this policy	5
Use of the reporting channel	6
When is the use of the reporting channel recommended?	6
For what is the reporting channel not intended?	7
How can concerns be reported?	7
Principles of this policy	8
Functions of the manager responsible for the reporting channel	9
External reporting channels	10
Approval, publication and review	10
Reporting Channel Procedure	11
Context	12
Who can make a report using the reporting channel?	12
What can be reported using the reporting channel?	12
How can a report be made?	13
What are the phases following the making of a report?	14
What guarantees does the reporting channel offer?	15
Protection of personal data	17
Annex	18
Data protection information	18
Reporting channel privacy policy	18





Context for the reporting channel

Puig¹ expects all Employees and other Stakeholders to uphold the high standards of Ethics and Compliance established in the Ethical Code.

To ensure accountability for these high standards, **Puig** promotes a Speak Up culture in which behaviour that may be unethical or breach internal or external regulations and laws can be reported.

The Reporting Channel supports this culture by providing a formal way to make a report through a clearly defined process with certain principles, rights, and guarantees.

¹ "Puig" refers to Puig Brands, S.A. company, and its subsidiaries and those other entities that may be incorporated in the future, with respect to which Puig Brands, S.A. holds or may hold (directly or indirectly) control, according to article 42 of the Spanish Commercial Code.

Purpose and scope of this policy

This Reporting Channel Policy develops the principles which govern the Reporting Channel, as part of the commitment of the Ethical Code to creating a transparent and ethical organization which encourages Employees and other Stakeholders to safely report potential breaches of the Code or regulations.

This Policy also protects Employees and other Stakeholders who make or handle reports using the Reporting Channel.

This Policy and the Reporting Channel Procedure have been approved by the Board of Directors of **Puig** Brands, S.A. and apply to all **Puig** companies and activities.

The various **Puig** divisions and local business units are permitted to develop this Policy and the Reporting Channel Procedure within a divisional or local policy and in such situations such divisional or local policy will comply with the terms, principles and behaviours contained within this Policy and the Procedure.

Within the Reporting Channel and according to the organizational needs of **Puig**, different channels can be implemented, as long as they comply with all the provisions established in this Policy and they are approved by the Manager Responsible of the Reporting Channel.



Use of the reporting channel

Any formal or informal channel can be used by Employees or other Stakeholders to report behaviours that may be unethical or that breach internal or external regulations and laws. However, the Reporting Channel <https://puigreportingchannel.ethicspoint.com/> can be used at all times, especially if other formal or informal alternatives are not appropriate due to the context or any other reason.

The Reporting Channel can also be used to ask questions about the Ethical Code and other internal or external regulations.

When is the use of the reporting channel recommended?

In general, the Reporting Channel should be used in cases of:

- Illegal activity or breaches of applicable law or regulations
- Behaviour which is contrary to the Ethical Code
- Breaches of internal **Puig** policies or regulations

The Reporting Channel Procedure provides details on the issues which should be reported using the Reporting Channel.



For what is the reporting channel not intended?

Some types of concerns are not normally expected to be reported through the Reporting Channel (except when they involve illegal activity, breaches of applicable law or regulations, behaviour which is contrary to the Ethical Code or breaches of internal **Puig** policies or regulations). They include:

- Disputes relating to terms of employment such as salary, benefits or performance appraisals.
- Personal grievances towards an individual or group (e.g., workplace conflicts).
- In general, any report not made in Good Faith, as defined in this Policy.

These concerns can be addressed with the line or functional manager or human resources. However, the Reporting Channel may always be used if the problem cannot be solved using other channels.

The Reporting Channel should never be used in emergency situations such as threats to life or property in which immediate assistance is required.

How can concerns be reported?

The Reporting Channel is operated by an independent third party (NAVEX) to ensure that the identity of the person making the report and that of any third party mentioned in the report is protected and remains confidential.

The Reporting Channel prevents access to your report by anyone without authorization, and guarantees information security, processing integrity and privacy of data.

Details on how the Reporting Channel operates can be found in the Reporting Channel Procedure that further develops this Policy.



Principles of this policy

The Reporting Channel is intended as a tool to create an environment in which everyone feels safe and protected when speaking up with their concerns. For this reason, the Reporting Channel incorporates the following principles, rights, and guarantees:

•◦ **Legality and integrity**

The Reporting Channel will be governed by applicable law, this Policy, and the Reporting Channel Procedure.

•◦ **Accessibility and availability**

The Reporting Channel will be made available via the tools, platforms and mechanisms established internally. Employees and other Stakeholders (both natural and legal entities) will have access to the Channel and be able to file reports 24 hours a day, 365 days a year.

•◦ **Traceability and independence**

Reports filed through the Reporting Channel will be registered and processed according to this Policy and the Reporting Channel Procedure. The Manager Responsible for the Reporting Channel will act independently of business functions and with the utmost respect for the regulations, principles and values of **Puig**.

•◦ **Anonymity**

The Reporting Channel allows anyone making a report to remain anonymous. Reports made anonymously will be treated in the same way as those made without anonymity.

•◦ **Good faith**

Information submitted through the Reporting Channel must be provided in Good Faith. Good Faith means that the person filing the report believes that the issue reported is unethical or illegal and that the facts reported are true at the time the report is made. Good Faith also means that reports are not made with malicious intent or for personal gain.



•◦ **Protection and non-retaliation**

Puig is committed to protecting anyone who makes a report of unethical or illegal conduct in Good Faith from any type of retaliation. Retaliation refers to any direct or indirect action or omission which causes or may cause unjustified harm. It includes but is not limited to dismissal, demotion or harassment.

•◦ **Transparency**

The Policy will be available publicly via the **Puig** website. Employees will be informed of and receive training on its contents.

•◦ **Right of defence and right to the presumption of innocence**

Puig guarantees the right of defence and right to the presumption of innocence of all persons involved in the reports, as well as any other corresponding right or guarantee according to internal regulations or legislations.

•◦ **Confidentiality**

The Reporting Channel ensures that all information filed, including the content of the report, shall remain confidential.

•◦ **Data protection**

External and internal data protection regulations will be respected, applying the data protection policies of **Puig** to the management of data obtained and/or processed through the Reporting Channel. Data subjects may exercise their data protection rights as indicated in the Privacy Policy of the Reporting Channel which is annexed to this Policy.

Functions of the manager responsible for the reporting channel

The Board of Directors, through the oversight functions assigned to the Audit and Compliance Committee, appoints the Chief Compliance Officer as the Manager Responsible for the Reporting Channel, with responsibility for the management and processing of reports as well as any other duties that may be assigned by applicable law.



Additionally, the Chief Compliance Officer shall report to the Board of Directors and the Audit and Compliance Committee annually and shall provide information regarding the Reporting Channel as required.

In the case of other reporting channels that may be implemented, the managers responsible for their operation will report to the Manager Responsible for the Reporting Channel.

External reporting channels

According to applicable law, there are countries in the EU where appropriate public authorities have been designated as ones to whom concerns about unethical or illegal conduct can be reported. These external reporting channels ensure accessibility and provide confidentiality and non-retaliation safeguards.

These external reporting channels are intended to be an additional option for anyone wishing to make a report and are not a substitute for the **Puig** Reporting Channel. The information related to the access to the external reporting channels will be reflected in the Reporting Channel platform and will be updated as soon as public authorities create them.

Approval, publication and review

This Policy and the Reporting Channel Procedure have been approved by the Board of Directors of **Puig** on 30 of May of 2023, coming into force at that time. In addition, they are published on the intranet, on the **Puig** website and will be communicated to the employees of **Puig** and to other stakeholders where applicable.

This Policy and the Reporting Channel Procedure may be reviewed and amended as required and they replace and supersede any previous policy or procedure as well as any previous reporting channel.

Non-compliance with this Policy and the Reporting Channel Procedure could result in the adoption of disciplinary measures as well as any other consequence provided for by applicable law.



Context

Puig provides a Reporting Channel managed by an independent third party (NAVEX), which allows those using the Channel to make reports in a structured, secure and confidential way. The Reporting Channel can be accessed using the following link
<https://puigreportingchannel.ethicspoint.com/>.

The principles which govern the Reporting Channel are set out in the Reporting Channel Policy.

Who can make a report using the reporting channel?

Anyone who detects a breach of the Ethical Code or applicable law can make a report using the secure and confidential Reporting Channel.

Puig employees who make reports using the Reporting Channel and others whom the law may specify are provided the guarantees of protection established by law and which are reflected in this Procedure.

What can be reported using the reporting channel?

Any breach of the **Puig** Ethical Code or applicable law can be reported using the Reporting Channel.

In general, the Reporting Channel is not intended to be used to report personal grievances or disputes relating to terms of employment. It would be better to address such issues through line or functional managers or human resources, although nothing prevents the use of the Reporting Channel in these cases also.

The Reporting Channel must not be used to report information in bad faith, either when the information is known to be false or for personal gain. The Reporting Channel should never be used in emergency situations in which immediate assistance is required.



How can a report be made?

Reports of potential breaches of the Ethical Code or applicable law can be made as follows:

- Preferably, reports should be made through the Reporting Channel platform: reports can be prepared in the Reporting Channel platform here <https://puigreportingchannel.ethicspoint.com/>.
- Additionally, as part of the **Puig** Speak Up culture, reports can be made in any way which is most convenient for the person making the report: for example, via other specific channels established in **Puig** such as customer support channels, in person or via email, preferably to the line or functional manager or human resources, or directly to the Manager Responsible for the Reporting Channel.

Reports received outside the Reporting Channel platform must be passed immediately to the Manager Responsible for the Reporting Channel, ensuring maximum confidentiality is maintained.

The Reporting Channel platform identifies other external reporting channels established by national authorities in the European Union which can be used simultaneously or alternatively.



What are the phases following the making of a report?

The phases that follow the making of a report are as follows:

- > **On receipt of the report by the Manager Responsible for the Reporting Channel**
 - The person making the report will be informed within seven days that the report has been received, providing this does not compromise the confidentiality of the information.
 - The report will be duly registered on the Reporting Channel platform, guaranteeing its confidentiality.
 - The content of the report will be analysed to determine whether it meets the requirements for admission, and this may involve requests for additional information or clarification of the information contained in the report to the person making it.
- > **Investigation**

Once the report has been admitted by the Manager Responsible for the Reporting Channel, the process of investigating the contents of the report will begin, if this is found to be necessary. During this phase, people may be selected to lead the investigation who are most appropriate to do so by virtue of their positions. These people may perform various functions, such as analysing documentation and carrying out interviews, amongst other actions.

The investigation will be carried out respecting the principles of impartiality, equality, independence, and honesty, and will conclude with the emission of a report prepared by those leading the investigation which will be passed to the Manager Responsible for the Reporting Channel.

This phase may not take longer than three months from receipt of the report, although if the facts reported are highly complex, it may exceptionally be extended to a total of six months.

- > **Decision**

Once the investigation is finalised the Manager Responsible for the Reporting Channel will prepare a draft decision which may include:



- The adoption of the most appropriate measures or actions given the nature of the facts reported and the degree to which they have been verified. The Manager Responsible for the Reporting Channel will communicate the measures or actions proposed to the corresponding area.
- The closure of the report when either the investigation has been unable to prove the facts reported, or the facts which are proved do not constitute an infraction or do not require the implementation of measures or actions.

•◦ Conclusion

Once the investigation is concluded:

- The appropriate communication measures will be taken.
- The implementation of the proposed measures or actions will be recorded.
- The personal data contained on the Reporting Channel platform will be saved and protected.
- A report will be made to the Audit and Compliance Committee and Board of Directors of Puig Brands, S.A.

What guarantees does the reporting channel offer?

Making a report via the Reporting Channel is accompanied by the following guarantees:

•◦ Confidentiality

The identity of a person making a report who wishes to be identified, as well as any third party mentioned in the report and any action taken within the context of the investigation, will be subject to maximum confidentiality. The Reporting Channel platform does not allow unauthorised access to information relating to reports.

The person making the report is guaranteed access to the platform via a unique username and password which allows them to monitor the progress



of their report, provide additional information, and communicate with the Manager Responsible for the Reporting Channel.

•◦ Anonymity

Reports may be made anonymously, although, to help the investigation of the facts reported, those making reports are encouraged to share their identity. A person making a report will always have the right for their identity not to be revealed to third parties.

•◦ Freedom from retaliation

Anyone who makes any form of report or consultation in good faith and in accordance with what is established in this Procedure is protected from any type of retaliation, discrimination, or penalisation as a consequence of the report made. **Puig** will sanction any type of retaliation made against anyone making a report in good faith.

Additionally, the following principles will be observed during the processing of a report:

•◦ Proportionality

The information gathered will be that which is strictly and objectively necessary to process the reports and prove the veracity of the facts reported and will always be treated as required by applicable data protection regulations. Unnecessary personal data will not be collected, and if it is collected inadvertently, will be eliminated as soon as possible.

•◦ Equality

All parties involved will be treated equally, regardless of factors such as hierarchical position or role.

•◦ Presumption of innocence and right to dignity

Each person will be considered innocent during the investigation process and their reputation and right to dignity will be respected.

•◦ Right to be heard and to self-defence

The person implicated by the facts reported will be informed of them, and every person involved in an investigation will be able to give their opinion with



respect to the facts reported and will have the right to ask for and present evidence to challenge them.

Protection of personal data

Information relating to the handling of personal data derived from the use of the Reporting Channel is annexed to this Procedure and can be found in the Privacy Policy on the Reporting Channel platform.



Annex

Data protection information

The personal data provided will be processed by "Puig Brands, S.A." as data controller in compliance with any regulation in force aimed at reporting potential breaches of applicable law as well as any breach of internal regulations, including **Puig** Ethical Code. Unless is it legally required, we will not disclose your personal information to any third party. Personal data means any information relating to an identified or identifiable natural person.

The parties involved may exercise their right of access, rectification, erasure, restriction of processing, right to object, portability under the terms established by law, by contacting data.privacy@puig.com. Please consult the Reporting Channel Privacy Policy for more information.

Reporting channel privacy policy

1. Who is the "Data Controller" of your personal data?

The entity responsible for the processing of personal data collected within the framework of this Reporting Channel is the parent company of **Puig**¹, Puig Brands, S.A., with address: Plaça Europa, 46-48, l'Hospitalet de Llobregat, 08902 Barcelona, Spain and Tax Identification Number A66674904. (hereinafter, "**Puig**").

In case you need to contact with the Data Protection Officer please contact in the following e-mail: data.privacy@puig.com .

2. For what purpose and legal basis do we process your personal data?

The Reporting Channel is intended for **Puig** employees or other stakeholders as defined by applicable law to report behaviours that may be unethical or that breach internal or external regulations and laws.

For legal purposes, it is hereby stated that the following purposes are pursued with this Reporting Channel, each of them with its proper legal basis:

¹ **Puig**" refers to Puig Brands, S.A. company, and its subsidiaries and those other entities that may be incorporated in the future, with respect to which **Puig** Brands, S.A. holds or may hold (directly or indirectly) control, according to article 42 of the Spanish Commercial Code.



a) To comply with any regulation in force aimed at reporting potential breaches of applicable law.

In the first place, we will process the information provided by the complainant or the one provided in the framework of the eventual investigation carried out in order to (i) manage and investigate the complaints submitted about possible breaches of regulations in force as well as any internal regulations, including **Puig** Ethical Code, and (ii) provide the legally established protection measures against retaliation, in compliance with the provisions of applicable law.

If the person reporting makes his complaint verbally and expressly requests to leave a record of it through a video recording (image and voice), **Puig** will obtain his/her consent to carry out this processing.

b) Attention and reply to possible consults, due to the legitimate interest of the person who makes them.

If a complaint is not filed, but simply a consultation (probably prior to a subsequent complaint), **Puig** will process the information received to attend, manage and give proper response.

The above will be carried out based on the legitimate interest of **Puig** and the person who makes the inquiry, without prejudice or harm to his or her privacy.

c) To comply with other legal requirements.

Finally, in some cases personal data may also be processed in order to comply with certain legal obligations that may be required of us. For example, if requested by a Court, or any State Security Force. In these cases, and as far as possible, we will inform you of this and the rule that enforces it.

This Policy can be adapted and/or developed by each **Puig** entity to meet the legal requirements set forth by local applicable law.

3. What personal data and information is collected and processed?

Puig may process personal information of the complainant and the reported person, as well as of third parties involved in the events that have been subject to a consult or complaint (e.g., possible witnesses). In this regard, it is not possible to define in advance which categories of personal data will be processed in this Reporting Channel, since it depends on the information that both the complainant, when filing his complaint, and the reported person, when defending himself, freely provide.



However, only the data strictly necessary to process the complaints and, where appropriate, to verify the reality of the events reported will be processed. Likewise, they will be adequate and not excessive in relation to the purposes indicated in paragraph 2 above.

In this sense, the complainant who wishes to reveal his or her identity must provide **Puig** with his or her current personal data so that the information contained in its files is updated and free of errors (in particular, the data through which **Puig** may contact him or her for any matter related to the complaint filed).

4. How long will we keep your data?

The personal data collected (through the complaint submitted and where appropriate, in the framework of the eventual subsequent investigation) may be kept only (i) for the time necessary to decide whether to initiate an investigation into the facts reported, (ii) where appropriate, during the time in which the relevant investigation is carried out and, finally, (iii) throughout the exercise of legal actions. In the case of a simple consultation, during the time needed for its processing and response.

If it is proven that the information provided or part of it is not truthful, it will be immediately deleted as soon as this circumstance becomes known, unless this lack of truthfulness may constitute a criminal offence, in which case the information will be kept for the time necessary during the legal proceedings.

In any case, if three months have elapsed since the receipt of the complaint without any investigation having been initiated, the information shall be deleted, unless the purpose of storage is to leave evidence of the operation of the channel. Communications that have not been followed up may only be recorded in anonymized form.

Finally, and after all of the above, the data collected will be kept to comply with possible legal obligations that may apply, as well as to meet possible claims and liabilities, keeping them properly blocked, and for the maximum periods legally established, available to the State Security Forces and Authorities, Courts, and possible relevant Public Administrations.

5. To which recipients will your data be disclosed?

Access to the personal data contained in the Reporting Channel will be limited, within the scope of their powers and functions, exclusively to:

- a) The Controller and whoever manages it directly.



- b) The human resources manager or the duly designated competent body, only when disciplinary measures may be taken against an employee.
- c) The person in charge of the legal services, if legal measures should be taken in relation to the facts described in the communication.
- d) The processors who may be appointed, as the case may be.
- e) The data protection officer.

If, as a result of the investigation process, the adoption of legal or disciplinary measures against the reported person is agreed, **Puig** will transfer the strictly necessary information to the **Puig** entity to which the reported person has a contractual relationship (of a labor or commercial nature, as applicable), in order to carry out and execute the relevant legal actions.

In this regard, the Data will only be transferred to **Puig** companies also from outside the EU for the same purposes referred to above. In this sense, the processing of data by other persons, or even their communication to third parties, will be lawful when it is necessary for the adoption of corrective measures in the entity or the processing of sanctioning or criminal proceedings which, where appropriate, may be applicable.

They may also be disclosed to those third parties to which **Puig** is legally enforced: for example, Courts and Tribunals, Security Forces and Authorities or any competent Public Body, upon their request.

Puig may also rely on the collaboration of third-party service providers, who may have access to such personal data and who will process them for and on its behalf. In relation to the above, **Puig** applies strict criteria for the selection of the suppliers, in order to comply with its obligations regarding data protection. Thus, and in accordance with the privacy terms under which these potential third-party suppliers will perform, **Puig** will, where possible, require them, among others, to apply appropriate technical and organizational measures, to process personal data for the stated purposes and only in accordance with **Puig**'s documented instructions, and to erase or return the data once the provision of the services has been completed.

The above is indicated considering that **Puig** may engage third party providers who perform their services, including without limitation, in the following sectors: legal advice, multidisciplinary professional services companies, or companies providing technology or computer services.

In these cases, the supplier must:



- Access solely in accordance with the written instructions that the Data Controller indicates to it for such purpose
- Not use data for any other purposes
- Implement the security measures -technical and organizational- necessary to ensure the confidentiality of the information to which it has access
- Not disclose to third parties the data to which it has access, not even for storage purposes.

6. Information to the parties involved

The parties involved in the inquiries or complaints received will be duly informed of the legal conditions regarding privacy under which their personal data will be treated. To carry out the above, **Puig** will arbitrate the necessary mechanisms to ensure that the recipients of this Channel can know and have at their disposal, in a simple, accessible, understandable and of course free of charge, the privacy rules contained in this Policy.

Likewise, every time a complaint or inquiry is made, **Puig** will inform in a particular way the parties involved of the collection and subsequent processing of their personal data. However, the means by which the above will be carried out will be managed on a customized basis. In this regard, in order to ensure compliance with this duty to inform, the following measures will be taken (depending on whether it is the complainant, the reported person or a third party involved):

a) Complainant

If the complainant identifies himself/herself when submitting the complaint, he/she will also be informed of the processing of his/her data in the communication sent to acknowledge receipt of the submission of his/her complaint or inquiry, with a link to this Privacy Policy. Exceptionally, this personalized notification will not be sent if the complainant has used a common or shared email account, or one that is accessible to more people in the organization (e.g., comercial@puig.com or compras@puig.com).

b) Reported person

As a general rule, the reported person shall be informed of the lodging of a complaint against him/her within a maximum of thirty (30) days from its receipt. However, it will be necessary to assess, on a case-by-case basis, whether informing him/her within such period could compromise the proper conduct and success of the investigation. In this case, if it is decided not to



inform the reported person at the initial stage of the investigation, such decision shall be duly documented and justified.

c) Any other interested party involved in the complaint or inquiry

Finally, third parties involved in the complaint or inquiry shall be informed prior to their involvement in the process: for example, a possible witness prior to his or her interview or statement being taken.

7. What are your rights when you provide us with your personal data?

The person reporting a complaint may exercise his/her right of access to personal data, as well as request for rectification of inaccurate data or, where appropriate, request its deletion when the data is no longer necessary for the purposes for which it was collected. You may also request the limitation and opposition of the processing of your data, in certain circumstances and for reasons related to your particular situation.

In the event that the person to whom the facts reported in a complaint refer exercises the right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate reasons that legitimize the processing of his or her personal data.

If the data subject has requested and given his or her authorization to the recording of his or her verbal complaint, he or she shall have the right of portability of such recording and may revoke his or her consent at any time, without retroactively affecting the processing of personal data carried out up to that time.

Such rights may be exercised under the terms established by law, in particular with a scope and content that does not allow the defendant to know, through its exercise, the identity of the complainant.

The user may exercise the aforementioned rights, under the terms and conditions provided for in current legislation, at **Puig**'s registered office or by sending an e-mail to compliance@puig.com.

In the event that you do not receive a satisfactory response and wish to make a complaint or obtain further information regarding any of these rights, they may contact the Spanish Data Protection Agency (www.agpd.es - C/ Jorge Juan, 6 de Madrid

However, in the event that the interested party who intends to file a complaint is not in Spanish territory, but in the State of any other member of the European Union, he/she may contact the Data Protection Authority of



the State in which he/she is located. To do so, you can find out which Authority to contact through the following link: [Data Protection Authorities and other institutions of interest](#)