

DATA PROTECTION POLICY OF THE INTERNAL INFORMATION SYSTEM

In accordance with the provisions set forth in Regulation (EU) 2016/679, of 27 April, on the Protection of natural persons with regard to the processing of their Personal Data (GDPR); in the Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD); and in Law 2/2023, of February 20, Regulating the Protection of Persons Reporting Regulatory Violations and the Fight against Corruption (Whistleblower Protection Act), as well as with the provisions of the rest of the applicable regulations on data protection, below we explain how we treat the personal data provided through the Internal Information System.

The Internal Information System has the necessary measures to guarantee and ensure the confidentiality of the identity and protection of the informant and any third parties mentioned in the communication, preventing access to the information to unauthorized persons.

1. DATA CONTROLLER

Your personal data will be processed by:

Information	Data of Data Controller
Company	J&C Prime Brands, S.L. (hereinafter referred to as the " Controller ")
VAT number	B58606203
Data Protection Officer (DPO) Contact	lopd@juveycamps.com

J&C Prime Brands, S.L., as the parent company of the group, will carry out the purposes identified in the section "Purposes" on behalf of the following companies of the group, in its capacity as Data Processor, based on a contractual execution:

Information	Data of the Co-Data Controllers
Company	Juvé y Camps, S.A.
VAT number	A08186025
DPO Contact	lopd@juveycamps.com

Information	Data of the Co-Data Controllers
Company	Anoia Industrial, S.L.
VAT number	B08237331
DPO Contact	lopd@juveycamps.com

Information	Data of the Co-Data Controllers
Company	Propietat D'Espiells, S.A.
VAT number	A08248247
DPO Contact	lopd@juveycamps.com

Information	Data of the Co-Data Controllers
Company	Distribuidora de Primeras Marcas, S.A.
VAT number	A58172685
DPO Contact	lopd@juveycamps.com

Information	Data of the Co-Data Controllers
Company	Pagos d'Anguix, S.L.
VAT number	B42142273
DPO Contact	lopd@juveycamps.com

2. IDENTIFICATION OF INTERNAL INFORMATION CHANNELS

The Data Controller has established the following internal information channels:

Channel	Contact information
<i>In writing (by any electronic means provided for that purpose)</i>	
Web form	https://juveycamps.c-etico.es/
<i>Verbally (via telephone or voice messaging system)</i>	
Face-to-face meeting	<i>(upon verbal request or through the authorized written channels)</i>

There is also the possibility of requesting a face-to-face meeting through any of the mentioned channels, which will take place within seven (7) days from the date of the request for a face-to-face meeting.

We inform you that the report may be made either anonymously or by name (providing the identity of the informant). However, it may be the case that the informant's identification data are essential to continue with the investigation of the complaint, so that failure to provide them may prevent the continuation of this.

External information channels:

You also have the possibility to file a complaint with the following competent whistleblower protection authorities, either directly or having previously communicated the complaint to any of the channels enabled by the Controller, if you believe that the complaint filed cannot be dealt with effectively or if you consider that there is a risk of suffering any retaliation:

- Spanish Independent Authority for Whistleblower Protection (AAI)
- Antifraud Office of Catalonia

3. PURPOSES

Depending on the processing carried out, personal data may be processed for the following purposes:

Purpose	Description of the purpose and legal grounds
Resolving queries	We will process the data to respond to queries made in relation to the operation and management of the Internal Information System and/or the Compliance Model. Legal Grounds: legitimate interest
Reception and processing of complaints	We will process the data to receive alerts or complaints, to decide whether to initiate an investigation of the alerts or complaints received, also for the purpose of conducting the corresponding investigation of the reported facts, to protect the informant from retaliation, to adopt, if necessary, appropriate corrective measures and, if necessary, to initiate legal action against the defendants and/or third parties.

	<p>If the communication of the alert or complaint is made verbally (by telephone, voice message or face-to-face meeting), we inform you that we are required to document the complaint in one of the following ways, at your option:</p> <p>(a) by a recording of the conversation in a secure, durable and accessible format; or</p> <p>b) through a complete and accurate transcript of the conversation made by the personnel responsible for handling the conversation.</p> <p>In the case of a transcription of the conversation, you will have the opportunity to verify, rectify and agree by signature to the transcription of the conversation.</p> <p>Legal Grounds: legal obligation</p>
<p>To prove the proper functioning of the Internal Information System and Compliance Model, and to keep evidence for the Company's defense.</p>	<p>We may retain your data to support the proper functioning of our Internal Information System, our Compliance Model and/or to preserve evidence for the Company's defense.</p> <p>Legal Grounds: legitimate interest and legal obligation</p>

4. TYPE OF PERSONAL DATA THAT MAY BE PROCESSED

Whether you provide us with your personal data directly or from a third party, we will process the following personal data:

Types of interested parties	Data categories
Consultant	Identification data of the consultant, contact data, employment data, economic data and other data associated with the query, evidence.
Nominative informant	Identification data, contact data, details of the facts considered relevant, evidence and voice.
<p>Anonymous informant</p> <p><i>(The informant may provide the following data or none of them)</i></p>	Pseudonym, contact information, evidence, voice.
<p>Confidential informant</p> <p><i>(The informant does not want the Responsible to know his identity. In this case, the identification data provided will be managed only by the external manager of the Whistleblowing Channel).</i></p>	Identification data, contact data, data associated with the reported conduct, evidence, voice.
Defendant	Identification data, data associated with the reported conduct, evidence.
Witness	Identification data, contact data, data associated with the reported conduct, evidence.
Third parties	Identification data, contact data, data associated with the reported conduct, evidence.

During the course of handling the communication sent by you, we may ask you to clarify the information communicated or request that you provide additional information.

5. LEGAL GROUNDS

We will process your data in accordance with one or more of the following bases of legitimacy mentioned above:

Legal Grounds	Description
Contract execution	We will process your data if this is necessary for the performance of a contract, to fulfil the obligations set out in the contract.
Legal obligation	We may also process your personal data because we are required to do so by law.
Public interest	We may also need to process your data for the performance of a task carried out in the public interest or in the exercise of public authority vested in us.
Legitimate interest	We may process your data when it is necessary for the satisfaction of overriding legitimate interests that we have in our capacity as Data Controller. For more information about the weighting of legitimate interests in each case, please contact the Data Protection Officer (DPO).

6. DATA COMMUNICATION

In general, your personal data will be kept confidential and will not be communicated neither to the persons to whom the facts reported refer nor to third parties.

However, your personal data may be communicated to those external service providers that we have contracted for the reception of information from the channel and, where appropriate, for the management and conduct of investigations that may be necessary, which will process the data in the capacity of Data Processor and, in no case, will process the data for their own purposes.

Likewise, they may be communicated to the Security Forces and bodies, Judges or Courts, as well as any other competent body in case of being required in compliance with the legislation in force.

When there are indications that the reported facts may constitute a crime, there is an obligation to immediately notify the facts to the Public Prosecutor's Office. If the reported facts may affect the financial interests of the European Union, in this case they must be referred to the European Public Prosecutor's Office.

7. INTERNATIONAL DATA TRANSFERS

Where the Controller has international suppliers or is part of a group of companies, your personal data may be processed outside the European Union or the European Economic Area.

In such a case, the Controller will ensure that such data processing is always protected by appropriate safeguards, which may include:

- EU-approved Standard Clauses: these are contracts approved by the European regulator and provide sufficient guarantees to ensure that the processing complies with the requirements established by the European Data Protection Regulation.
- Third-party certifications: framework agreement between the EU and a third state that establishes a standardized framework for data processing in accordance with the requirements of the European Data Protection Regulation.

8. DURATION OF PROCESSING

- **Inquiries**

In the case of inquiries, personal data will be kept for the time necessary to resolve the query or issue raised and provide the answer to the person concerned. Once the corresponding retention period has expired, the data may be duly blocked and retained to prove compliance with the Compliance Model of the Data Controller and, where appropriate, to comply with legal obligations. Once this period has expired, the data will be definitively deleted.

- **Complaints**

Personal data will be kept in the Internal Information System only for the time necessary to decide whether to initiate an investigation into the facts reported and, in any case, a maximum period of three (3) months from the date of sending the acknowledgement of receipt or, if we have not provided an acknowledgement of receipt, a maximum period of three (3) months from seven days after sending the complaint.

If after three (3) months from the receipt of the complaint no investigation actions have been initiated, the data will be deleted from the Internal Information System, unless they are kept as evidence of the proper functioning of the system, in which case they will be anonymized, without the obligation of blocking provided for in the LOPDGDD being applicable.

Data Retention of admitted complaints:

The personal data of the complaints admitted for processing will be kept blocked within the Internal Information System for the duration of the investigation and, in general, for the following purposes:

1. up to a maximum period of ten (10) years, once the established maximum conservation period has expired, they will be definitively destroyed in compliance with the provisions of the Whistleblower Protection Law.
2. to prove the effective operation of our Compliance Model, we may keep them for a longer period, in accordance with the provisions of Article 31 bis of the Criminal Code.
3. when the reported fact constitutes a crime or administrative infraction during the statute of limitations period for crimes and administrative sanctions established in the Penal Code or in the laws applicable to each case.

We also inform you that we will immediately delete personal data in certain cases, without any obligation to block the data:

- if it is proven that the information provided or part of it is not truthful, unless the lack of truthfulness constitutes a criminal offense, in which case the data will be stored for the necessary time during the legal proceedings.
- if personal data that have been communicated are not necessary for the knowledge and investigation of the actions or omissions within the scope of this whistleblowing channel, including special categories of data. In the latter case, the data will be deleted immediately, without the registration and processing of such data.

9. EXERCISE OF RIGHTS

The owner of the personal data may at any time exercise his/her/them data protection rights (including withdrawal of the consent granted) of access, rectification, deletion, opposition, portability and limitation free of charge by writing to Carrer Sant Venat 1, 08770 Sant Sadurní d'Anoia (Barcelona) and including the reference "Datos Personales J&C Prime Brands".

In the event that we consider it necessary, i.e. that it is you who is exercising the corresponding data protection right, we may request a copy of your ID card or equivalent document proving your identity in order to execute your request to exercise your rights.

However, if the person under investigation exercises the right to oppose the processing of his personal data, it will be presumed that, unless evidence to the contrary is provided, there are compelling legitimate reasons that legitimize the continued processing of his personal data.

If you have any questions or complaints about how we handle your personal data, you can contact our DPO, through his contact address indicated in the "**Data Controller**" section.

Additionally, you may file a complaint before the Spanish Data Protection Agency (www.aepd.es) if you believe that we have not properly addressed your rights.

10. ADDITIONAL INFORMATION

For more information on how to exercise your data protection rights, please refer to our web Privacy Policy which can be found at www.juveycamps.com.

Last update: 29th June 2023