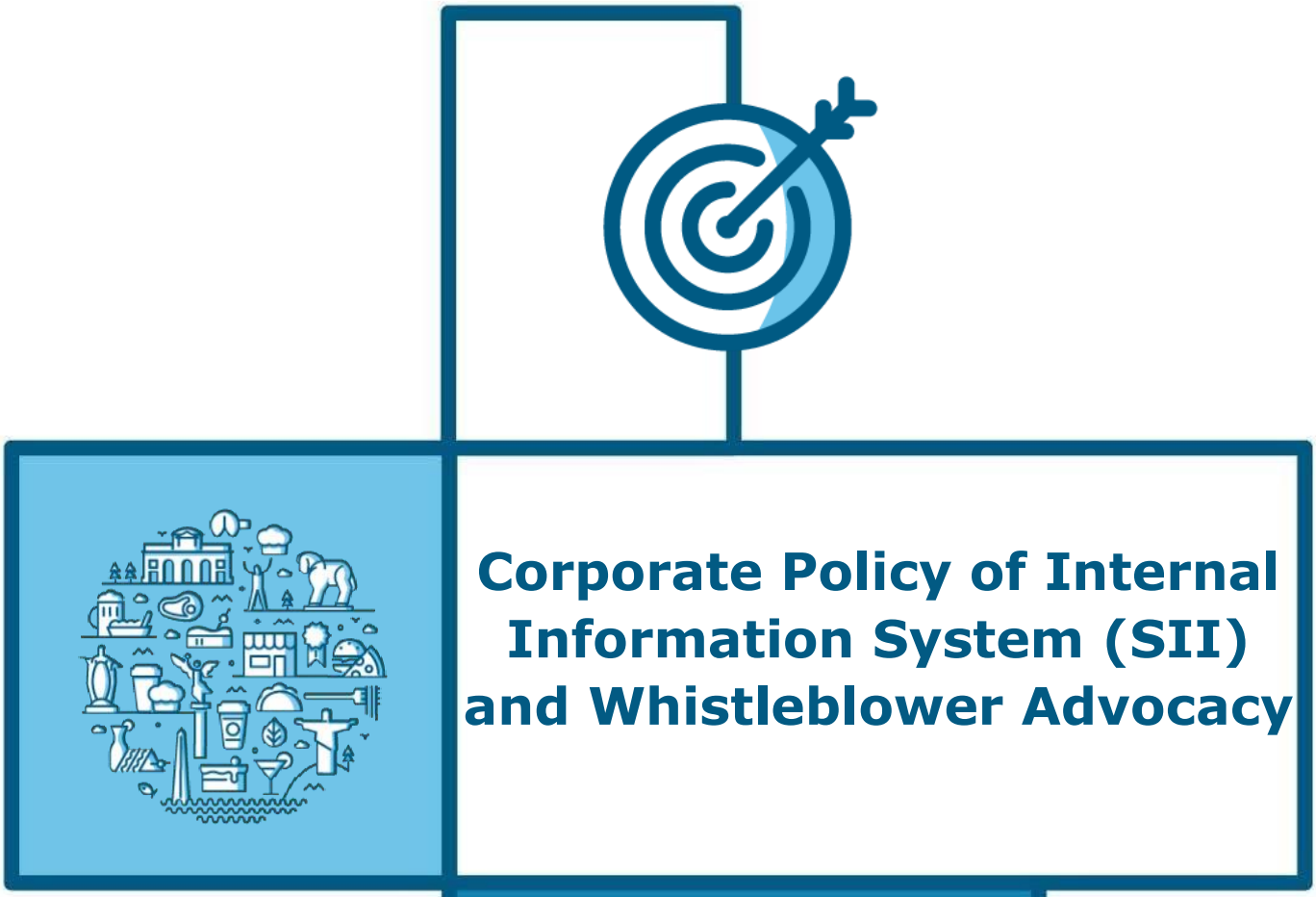
Alsea



Corporate Policy of Internal Information System (SII) and Whistleblower Advocacy

POL-CUMP-EUR-022

General Description of the Document	
Document Title:	Corporate Policy of Internal Information System (SII) and Whistleblower Advocacy
Area:	Compliance
Macro-process:	Regulatory Framework - Corporate Policies
Process:	Compliance and Risk Management
Sub-process:	Compliance
Scope:	Europe
Version:	01
Date of last version:	07/06/2024
Prepared by:	Compliance Officer Alsea Europe
Reviewed by:	Compliance Committee Alsea Europe
Approved by:	Board of Directors of Alsea Europe
Verified for Internal Control:	Compliance Committee Alsea Europe

Version register								
Version	1	2	3	4	5	6	7	8
Date	07/06/2024							

Content

1. Objective

As stipulated by the Alsea Europa[1] (hereinafter, "***Alsea Europa***", the "***Company***" or the "***Group"*** indistinctly) Code of Ethics and Professional Conduct, each and every employee[2] working at Alsea Europa and those third parties with which Alsea Europa maintains commercial or professional relationships must display integrity and carry out their activities in accordance not only with the legal framework but also with Alsea Europa's internal regulations.

Similarly, the aforementioned persons and entities hold the duty, within the scope of preventing and detecting irregular or unlawful conduct, to report any alleged irregularities or acts contrary to the law or the internal rules that they become aware of.

Hence, Alsea Europe has established an Internal Reporting System (hereinafter "**SII**") in accordance with the requirements set out in the legislation applicable to the companies comprising Alsea Europe and correspondingly transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law (hereinafter "***Directive 2019/1937***")[3].

This Corporate Policy of Internal Information System (SII) and Whistleblower Advocacy (hereinafter, the "***Policy***"), approved by the Board of Directors of FOOD SERVICE PROJECT, S.A. (hereinafter, "***FSP***"), on the one hand, demonstrates the clear commitment of Alsea Europe to ensuring good corporate governance practices and to developing a culture of ethical and regulatory compliance, which thereby promotes and strengthens among its stakeholders -both internal and external- a culture of information and communication as the mechanism enabling ALSEA EUROPE to appropriately prevent and detect irregular conduct and, thus, to be in a position to react. In addition, this furthermore establishes the rules and general principles regulating the SII and thereby consisting of the set of human, material and economic resources deployed to ensure: (i) the protection of Whistleblowers reporting breaches within framework applicable by this Policy, and (ii) their appropriate and effective treatment.

2. The Internal Information System (SII)

Alsea Europe's SII: (i) is allocated a specific manager; (ii) integrates the different internal information channels established throughout the Company; (iii) includes specific procedures for the Management of Information Received (hereinafter, the "***Procedure***") which, in order to promote the internal information culture, guarantees the protection of informants and has received approval from the FSP Board of Directors; and (iv) is independent of the internal information systems of other entities and bodies.

---

[1] For the purposes of this document, the "Alsea Europa" group of companies is understood to include both FOOD SERVICE PROJECT, S.A. (FSP) and those companies - currently or in the future - in whose share capital FSP holds, directly or indirectly, a majority of the shares, holdings or voting rights or, alternatively, when it has appointed or has the power to appoint a majority of the governing or administrative body members in such a way that it effectively controls the company.

[2] For the purposes of this Policy, staff are defined as all employees who provide services to the companies making up Alsea Europe.

[3] For the purposes of this Policy, the legislative frameworks applicable to the companies comprising Alsea Europe in this matter are: (i) Belgium: The 28 November 2022 law on the protection of whistleblowers of breaches of national or European Union law occurring within a private sector entity, which entered into force on 15 February 2023; (ii) France: Law No. 2022-401 of 21 March 2022 enacted to improve the protection of whistleblowers; (iii) The Netherlands: the Dutch law transposing the Directive partially entered into force on 18 February 2023; (iv) Luxembourg: the 16 May 2023 law transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law; (v) Portugal: Law No. 93/2021 of 20 December 2021; and (vi) Spain: Law 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption.

3. Related documents

Code	Name of the document
POL-CUMP-EUR-001	Code of Ethics and Professional Conduct
POL-CUMP-EUR-002	Corporate Anti-Corruption Policy
POL-CUMP-EUR-003	Corporate Policy Conflict of Interest
POL-RH-EUR-001	Occupational Risk Prevention Policy
POL-AJ-EUR-001	Corporate Data Protection Policy
POL-CUM-EUR-003	Corporate Gift and Invitation Policy
POL-CUMP-EUR-005	Corporate Risk Management Policy
POL-CUMP-EUR-006	Corporate Compliance Policy
PRO-CUMP-EUR-009	Procedure for the Management of Information Received

4. The Internal Information System (RSII) and Internal Information Channel Managers (CII)

The FSP Board of Directors has appointed the Compliance Committee (hereinafter, the "***RSII***") as the body responsible for supervising and managing the RSII which, as a collegiate body, shall then appoint a Internal Reporting Channel manager (hereinafter, the "***CII Manager***") from among its members.

The monitoring, supervision and interpretation of this Policy and the Procedure, without infringing on the powers reserved to the FSP Board of Directors, remains the responsibility of the RSII. Furthermore, the latter shall also be responsible for ensuring compliance and, when the occasion arises, for their interpretation and updating, whenever either appropriate or in the event of changes to the organisational and control structure, the activities undertaken and/or to the legislation or jurisprudence.

Notwithstanding the foregoing, the CII Manager, within the framework of his/her functions and without prejudice to the powers of the RSII, may develop such rules or guides for implementing this Policy and Procedure as and when deemed necessary to ensuring the appropriate functioning of the SII.

5. Dissemination

5.1. Subjective scope of application

Alsea Europe has set up its SII as a public communication channel available to:

(i) anyone who works or has worked in the different companies that make up Alsea Europe (e.g.: managers, employees, interns, trainees, etc.); or
(ii) anyone who is or has been a member of its administrative or executive bodies; or
(iii) anyone who interacts or has interacted, in all or part of the business process, with or without participation in Alsea Europe obtaining its objectives and results; or
(iv) external parties who have had, have or may have a direct relationship and a legitimate and reasonable commercial and/or professional interest (shareholders, customers, suppliers and their employees, franchisees and their employees, volunteers, etc.).

All of them are hereafter collectively referred to as the "***Informants***".

5.2. What should be reported through the Internal Information System (SII)?

The SII is not a complaints or suggestions box but rather a system designed to: (i) dissuade potential non-compliers; (ii) guarantee that all potentially irregular actions can be reported and, when necessary, duly investigated; (iii) resolve doubts; and (iv) establish the necessary

measures to ensure the protection of those who collaborate with reporting and informing of possible offences.

In view of the foregoing, through the SII, informants may report actions or omissions constituting infringements or non-compliances occurring in a labour or professional context and related to any of the companies making up the Group across the following areas:

(i) Infringements of EU and local laws applicable to Alsea Europe:

a) Infringements of European Union (EU) law, provided that they:

- impact on matters such as: public procurement; financial services, products and markets, and the prevention of money laundering and terrorist financing; product safety; transport safety; environmental protection; consumer protection; and the protection of both privacy and personal data and of networks and information technology systems;
- constitute fraud or illegal activity affecting the interests of the European Union; or
- affect the internal market[4], including infringements of EU competition rules and Member State granted aid as well as infringements concerning the internal market in relation to actions breaching corporate tax rules or practices aimed at obtaining tax advantages that defeat the object and purpose of corporate tax law.

b) Criminal offences; and

c) Minor, serious or very serious administrative infringements.

In any and all cases, this shall include all offences relating to workplace harassment, sexual or gender based harassment, and offences relating to workplace health and safety as well as administrative offences involving financial losses to the Treasury and/or to the Social Security system.

The aforementioned criminal and administrative offences are stipulated according to the provisions of the local laws applicable to Alsea Europe.

(ii) Other compliance irregularities that do not fall under these auspices (i), in particular those related to non-compliance with Alsea Europe's Code of Ethics and Professional Conduct or any other internal Alsea Europe rules (e.g. policies, protocols, etc.).

(iii) Consultations on regulatory compliance.

All communications on infringements and all queries submitted through the SII are received by the CII Manager. The CII Manager holds responsibility for managing them in accordance with the Procedure for the Management of Information Received.

Thus, following the implementation of the Internal Information Channel (hereinafter, the "***CII***"), the following channels are integrated into the SII and are correspondingly no longer operational:

a) The Whistleblower Channel, deactivating the e-mail address canaletico@alsea.net;

b) The Data Protection Channel dpd@alsea.net for data protection breaches and violations.

[4] The internal market comprises a geography without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.

5.3. What communications are excluded from the Internal Information System (SII)?

As stated above, this does not provide a mailbox for complaints or suggestions and should be used responsibly and for its respective intended purposes and, therefore, the following should not be communicated through the SII:

a) General information related to Alsea Europe.
b) Complaints of a commercial or billing type.
c) Matters for which there are specific channels (customer service, exercise of ARCO-POL rights, etc.).
d) Doubts, queries, claims and complaints of a labour or salary related nature.
e) Complaints about either the facilities or their state of repair.

To this end, the regular channels shall continue to be available for communications, requests, queries or observations relating to, among others, the following:

- The Exercising of ARCO-POL Eights[5].
- Customer Service.
- External Communication.
- Requests for Invoices.
- Talent and Selection.
- Employment Channels.
- Franchise Applications.

Information communicated through these channels will continue to be managed through the existing channels and means and in accordance with their own specific procedures.

6. Types and means of communication

6.1. Types of communication

6.1.1. Consultations

The purpose of these consultations may be either to suggest changes or improvements or, where appropriate, to raise questions regarding Alsea Europe's Code of Ethics and Professional Conduct, any other Alsea Europe internal rules or the legislation applicable law, or whenever such application is in doubt as well as any and all issues related to compliance and/or the crime prevention rules.

Any concerns relating to courses of action or conducts that might impact on compliance and/or crime prevention rules should also be submitted for due consideration.

6.1.2. Complaints

The purpose of whistleblowing is to report any risks or actual breaches of the applicable regulations, whether internal or legal in nature, and especially for reporting any alleged committing of crimes as indicated in section 5.2 of this Policy. This channel of communication may therefore serve to report offences or breaches either already committed or foreseeable on the basis of reasonable indications and as well as the existence of any hitherto undetected risks that might facilitate criminal action.

6.2. Means of communication

Communications may be submitted through the following channels:

a) As the priority means, through the link Alsea Europe provides informants on its corporate website.

[5] *The rights of access, rectification, cancellation, opposition, portability, suppression and limitation as regards data protection*.

b) By postal mail delivered to Camino de la Zarzuela, 1, Madrid (28023) Spain, for the attention of the CII Manager.

c) Upon the request of Informants, in person, either by hand-delivery of the written complaint or verbally, at the address corresponding to Camino de la Zarzuela, 1, Madrid (28023) Spain, to the CII Manager, who will then be responsible for determining the conditions according to which delivery takes place in order to preserve confidentiality; and, in the case of verbal communications, to collect them in writing, together with the signatures of Informants. An online meeting with the CII Manager may also be requested.

d) Applicable exclusively for cases of workplace, sexual or gender-based harassment, the complaint may be submitted, at the employee's choice, to the bodies established for this purpose by the Procedure for preventing and dealing with instances of moral and sexual harassment applicable to the Group at the local level (for example, the Instructing Committee for Dealing with Situations of Harassment, the doctor assigned to the prevention service, legal representatives of employees in the workplace).

All communications, regardless of the channel by which they are made, must be delivered to the CII Manager, who will then be responsible for handing them on the CII for their subsequent management in accordance with the provisions of this Policy.

7. Content of communications

7.1. Consultations

The consultation should specify which specific aspects of Alsea Europe's Code of Ethics and Professional Conduct, or any other internal rules or applicable law, have raised questions over their of interpretation and/or applicability, changes or improvements.

7.2. Complaints

In order for the complaint to be admissible, the following points should all, as far as is possible, be clearly indicated:

- Relationship with Alsea Europe of the Informant: Collaborator, Supplier, Franchisee, Client, etc..
- A clear and detailed description of the incident or of the potentially irregular conduct, paying particular attention to:
  - ✓ Date or period of the events.
  - ✓ Means of committing the possible/alleged unlawful conduct.
  - ✓ Whether there are other persons able to provide further information or corroborate your testimony.
  - ✓ The business area or company affected.
- Where possible, identification of the persons presumed responsible for the irregularity or, failing that, indication of the details enabling the identity of the person(s) presumed responsible.
- If available, documents or evidence related to the events surrounding your report.
- A declaration by Informants that they have read the data protection notice and are duly informed about the processing of their personal data in accordance with the provisions of **Annex I**.

Informants are furthermore warned that they should try to provide the information required to report a certain fact and avoid providing excessive or unnecessary data (e.g. documents obtained irregularly or owned by a third party, documents that are not directly related to the facts reported, etc.). If the report does not contain the information required to initiate an investigation, additional or complementary information or documentation may be requested from Informants prior to its acceptance for processing.

Complaints relating to information excluded from the scope of the SII shall not be admissible.

7.3. Prohibited information

All communications that run counter to the legal system are excluded from the SII, including those relating to classified information and professional secrecy, for example, those stipulated for the legal profession and the confidentiality of the Security Forces and other entities within the scope of their respective actions.

8. The Procedure for Managing the Information Received

All the Enquiries and Complaints received are managed and processed in accordance with both the applicable regulations and the provisions handed down in the Procedure.

As all compliance violations are subject to the SII and are therefore handled in accordance with the provisions of the Procedure, the current version of the Alsea Europe Complaints Channel Operating and Management Protocol is thereby replaced and superseded by the current version of the Alsea Europe Complaints Channel Operating and Management Protocol.

In addition, the aforementioned Procedure shall include the rules established on workplace, sexual or gender-based harassment that may be included in any Procedures for the prevention and treatment of situations of moral and sexual harassment that may be applicable to the Group at the local level.

8.1. Principles

The Procedure developed in this Policy is based on the principles of trust, proportionality, impartiality, truthfulness and confidentiality; on the right to honour, to the presumption of innocence, to defence, to non self-incrimination and to the effective protection of the rights of both the informant and the person under investigation; as well as protecting the informant against potential reprisals.

Under no circumstances may the Procedure violate the rules governing criminal proceedings, including their preliminary investigation.

8.2. Managing the information received

All information communicated through the SII, regardless of the channel or medium applied, will be received by the CII Manager.

The CII Manager is therefore responsible for deciding on: either (a) the admission and processing or archiving of the information received; or (b) the referral to the relevant manager for processing or archiving and in accordance with the Procedure in either case.

Reports of harassment (workplace or sexual) shall be received by the CII Manager. In the event of a criminal offence, the reporting is handled by the CII Manager and, in the event of an administrative offence, by the body the Procedure potentially establishes for this purpose of the prevention and treatment of moral and sexual harassment situations applicable to the Group at the local level (e.g.: the Committee for the Investigation of Incidences of Harassment (CITSA)). In any case, the processing applicable to this information shall stem from the Procedure.

Within seven (7) calendar days of receipt of the information, the CII Manager shall deliver acknowledgement of receipt to the Informant.

The CII Manager, after sending acknowledgement of receipt, will then decide on the admissibility, inadmissibility or the referral of the information to the competent manager in keeping with the subject matter. In the event of admission, the investigated party or parties shall be notified in accordance with the provisions of the Procedure. In no case will the identity of the Informant ever be communicated to the person or persons under investigation, nor will the latter receive access to the communication/complaint. In any case, Informants are subsequently notified of the admission or closure of their reports.

The CII Manager holds responsibility for the investigation who, depending on the subject matter of the report, may delegate this in whole or in part to other members of the organisation and/or to external advisors, as may be the case for investigations into serious criminal offences, which may be outsourced to specialised external consultants.

Resolving the investigation may not exceed three (3) months from acknowledgement of receipt of the communication or, should no acknowledgement of receipt have been sent to the Informant, three (3) months on from the expiry of the period of seven (7) days following receipt of the report, except in cases of particular complexity in which the investigation may be extended for a maximum of three (3) additional months.

These time limits shall be reduced in cases of workplace, sexual or gender-based harassment in order to comply with the time limits that may be established in this respect by procedures for the prevention and dealing with incidences of moral and sexual harassment applicable to the Group at the local level.

Once this investigation has been completed, the body that has carried it out will issue and, whenever necessary, share a final report with the CII Manager detailing the conclusions of the investigation.

In cases of workplace, sexual or gender-based harassment, once the investigation has been completed by the competent body and in accordance with the Procedure, the competent body shall adopt any measures that may be appropriate in accordance with the procedures for preventing and dealing with situations of moral and sexual harassment applicable to the Group at the local level.

Should the conclusions of the final investigation report indicate that this involves a presumed criminal act for which the Group may be directly criminally liable, the final report shall be sent to the RSII, who shall then decide on what disciplinary and/or legal measures are to be adopted as well as any eventual notification to the competent judicial authorities and/or the Public Prosecutor's Office or the European Public Prosecutor's Office should the facts impact on the financial interests of the European Union.

The SII shall maintain a register of all information received, assigning an identification code to each file. This register shall not be made public.

8.3. Whistleblower Rights and Guarantees

Informants who report breaches as described in section 5.2 of this Policy shall be entitled to the following rights and safeguards:

a) Decide whether or not the communication is made anonymously. In the event the Informant chooses the non-anonymous option, the confidentiality of his/her identity will nevertheless be guaranteed both by the RSII and by the CII Manager and the persons who, where appropriate, intervene in processing the information.

b) Formulate the communication in writing and/or verbally. The authorised CII deploys a mechanism that prevents its identification by third parties.

c) Be notified of the status of the processing and outcome of their reports. Therefore, Informants may choose to receive notifications or communications relating to the admission and processing of the information or expressly waive this right. In the event of opting to receive notifications, the Informant may then choose whether or not to maintain an anonymous dialogue.

d) Appear before the CII manager on his/her own initiative or when requested to do so by him/her, with the assistance of a lawyer should such be necessary.

e) Exercise the ARCO-POL rights regarding the protection of personal data.

8.3.1. Right to confidentiality

The SII guarantees the confidentiality of the identity of the Informant and of any third party mentioned in the communication, as well as the actions carried out in managing and processing

their reports. This also guarantees data protection and the prevention of access by unauthorised persons.

Likewise, whenever a report is submitted to the SII, whether a Query or a Complaint, sent through a channel other than the CII or is submitted to other employees or representatives other than the RSII or the CII Manager, they are obliged to guarantee confidentiality and report it immediately to the CII Manager for processing. Failure to comply with this obligation on behalf of employees or representatives shall be classed as a very serious breach of this Policy and, therefore, a breach of their employment and contractual obligations.

The identity of Informants may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctionary investigation. Disclosures made under this paragraph shall be subject to the same safeguards as laid down in the applicable regulations. In particular, Informants shall be informed prior to their identities being revealed unless such communication might jeopardise the investigation or judicial proceedings.

8.3.2. Right to anonymity

Informants may decide to make anonymous reports and the SII guarantees anonymous access to the CII both for making the initial complaint and for communicating with Alsea Europe whenever deemed necessary in keeping with the contents of the case opened as a result of the complaint.

8.3.3.Prohibition of reprisals

Adopting any form of retaliation, discrimination and penalisation against any Whistleblower is strictly forbidden, who, in good faith and with reasonable grounds to support the same, brings to the attention of Alsea Europe, through the SII, the alleged committal of conduct falling within the SII scope of application. This guarantee also extends to any person participating in the investigation (e.g. witnesses, injured parties, etc.), provided their interventions are made in good faith.

Retaliation is understood to be any act or omission that is prohibited by law and/or that, directly or indirectly, entails unfavourable treatment for the person/s who experience this in working or professional contexts solely because of their status as Whistleblowers; provided that such action or omission occurs either during the investigation phase or within two (2) years of its completion. An exception is made in cases where such actions or omissions can be objectively justified in terms of a legitimate purpose and where the means deployed to achieve such a purpose are necessary and appropriate.

In the event of any breach of this guarantee, this must be reported for investigation and, whenever confirmed, the perpetrator of reprisals may be subject to disciplinary action.

Those who communicate are expressly excluded from the protection provided for in this paragraph whenever:

a) Information has been previously communicated through the CII and rejected.
b) Information relating to claims of interpersonal conflicts or affecting only the Reporting Person and the persons to whom the communication or disclosure relates.
c) Information which is already fully available to the public or which constitutes mere hearsay.
d) Information relating to actions or omissions not covered by section 5.2 of this Policy.

Those who have reported information about breaches referred to in section 5.2 of this Policy anonymously, but have subsequently been identified and do not fall within the exclusion criteria referred to above, are entitled to full protection against retaliation.

8.3.4.Acting in Good Faith

Should the investigation determine that the report is false and that the Whistleblower acted with knowledge of its false nature or with reckless disregard for the truth, criminal or civil liability and/or the appropriate disciplinary measures may be applied in accordance with the

terms contemplated in the current legislation and the disciplinary regime of Alsea Europe, and consequently also eventually waiving the requirements of confidentiality.

The submission of reports to the SII in bad faith is not an acceptable practice and misuse of this system will be prosecuted.

Within this framework, Informants are considered to be acting in bad faith whenever they:

- Are aware of the falsity of the facts.
- Act with blatant disregard for the truth.
- Act with intentions of revenge and/or harm towards the person or company subject to the report.
- Act with intentions of undermining the honour or the professional, business or professional reputation of any person associated with Alsea Europe.

8.4. Rights of the Investigated Party

Persons under investigation retain the right to be presumed innocent, to act in their own defence and may access the investigation file as well as the effective protection of their rights. To this end, they shall be provided with a brief account of the facts under investigation, the right to refute any allegations and to submit whatever evidence they consider necessary in their own defence. While entitled to access the investigation file, under no circumstances shall the identity of informants be communicated to persons under investigation nor shall they be authorised to directly access the complaint. Likewise, persons under investigation may be assisted by a lawyer.

Persons under investigation shall be entitled to the same confidentiality as that established for Informants, preserving their respective identities and the facts and data in the investigation file.

8.5. Conflicts of interest

In the event that information communicated through the SII relates to the RSII or the CII Manager and/or any other person who may intervene in its management and processing, their abstention and absolute prohibition against intervening in the processing (admission, investigation and resolution) of the investigation is to be guaranteed as duly stipulated by the Procedure.

9. External channels

The SII implemented by Alsea Europe constitutes the preferred channel for reporting the actions or omissions set out in section 5.2 (i) of this Policy, provided that the Reporting Person considers that the breach can be dealt with effectively and there is no risk of retaliation. **Annex II** of this Policy lists, by way of examples but not exclusively, certain external channels in the countries in which Alsea Europe operates for such purposes. Notwithstanding the foregoing, Alsea Europe employees are nevertheless required to report through the SII any breach of the internal rules set out in section 5.2(ii) where it does not constitute a breach of the rules set out in section 5.2(i).

9.1. Cooperation with the authorities

Alsea Europe, provided that its right of defence and the right against self-incrimination are not compromised, will cooperate and/or respond with the utmost diligence to any and all requests made by the administrative and judicial authorities, the Public Prosecutor's Office or the European Public Prosecutor's Office in relation to actions related to Alsea Europe or for any other reason. Meeting these requirements falls within the scope of the responsibilities of the Compliance Committee, which must immediately inform the FSP Board of Directors whenever the facts triggering the making of such requests may result in direct criminal liability for the Group.

10. Protection of Personal Data

The SII management is to comply with the applicable legal regulations on the protection of personal data for which purpose "Information on the processing of personal data" is provided in ***Annex I***.

11. Non-compliance

Any breach of this Policy by Alsea Europe employees will be analysed in accordance with internal procedures, legal regulations and the agreements in effect and, whenever applicable, the corresponding disciplinary measures will be applied to offenders, without prejudice to any other liabilities (criminal or otherwise) they may have incurred.

12. Dissemination and Approval

This Policy is available to all Alsea Europe members of staff, as well as to third parties, through its publication on the corporate website.

Alsea Europe will take the necessary measures to disseminate, train and inform all its employees about the SII, its principles, guarantees and obligations, as well as its purpose.

This Policy has been approved by the FSP Board of Directors on 07 of June of 2024 and enters into effect as of that date.

ANNEX I. Information on the Processing of Personal Data

BASIC DATA PROTECTION INFORMATION (FIRST LAYER)

Data controller: FOOD SERVICE PROJECT, S.A.

Purpose: To manage the information processed through the CII.

Rights: You may exercise, where appropriate, your rights of access, rectification, deletion, opposition, portability, limitation, as well as the right not to be subject to automated individual decisions, by writing to dpd@alsea.net or to the postal address Camino de la Zarzuela, 1. Madrid (Spain). You may also lodge a complaint with the competent supervisory authority for data protection.

Additional information: You can consult additional and detailed information by clicking on the "Privacy Policy" established for this specific processing.

PRIVACY POLICY AND ADDITIONAL DATA PROTECTION INFORMATION (SECOND LAYER)

1. Data Controller and contact details for the Data Protection Officer

In accordance with personal data protection regulations, FOOD SERVICE PROJECT, S.A. with Tax Identification Code A-82798943 and headquartered at Camino de la Zarzuela, 1 - 28023, Madrid, will be considered the data controller (hereinafter, indistinctly, the "**Controller**" or "**FSP**") as the holding company of the group of companies known as Alsea Europa[6] , with FSP therefore responsible for the roles played by the Internal Information System Manager (hereinafter, "**RSII**") and the Internal Information Channel Manager (hereinafter, "**CII Manager**") of Alsea Europa, the internal Alsea Europa bodies that hold responsibility for the correct operation of the Internal Information System (hereinafter, "**SII**") and the management of the Internal Information Channel (hereinafter, "**CII**").

Interested parties may contact Alsea Europe's Data Protection Officer by email at dpd@alsea.net.

2. Purposes and lawfulness of processing

Personal data accessed in the performance of the functions and procedures regulated in this Policy shall be governed by the provisions of 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 (hereinafter "**GDPR**") and the local laws transposing the regulation.

In cases where Informants choose to submit a complaint anonymously, FSP will not process any personal data unless you choose to disclose it voluntarily. While the Controller strives to ensure your anonymity, please note your identity may be inferred based on the specifics of the complaint.

If you choose to disclose your identity, FSP will process your personal data for the purpose of processing and responding to the complaints received.

The legitimate grounds for this processing depend on the nature of the complaint filed. Specifically, when the complaints **(i)** refer to activities or omissions classified in the national law transposing Directive (EU) 2019/1937 or which may be classified as criminal offences or serious or very serious administrative offences, the processing takes place based on the existence of a legal obligation, and is therefore subject to the provisions of Article 6.1.c) of the GDPR; **(ii)** when referring to offences other than the above but stemming from "acts or conduct that may contravene the applicable general or sectoral regulations" (e.g. minor offences), the basis for the legitimacy of the processing arises from the public interest as established in the

[6] *For information on the companies that make up Alsea Europe, please consult section 1 (Identification data) of the Legal Notice at https://europe.alsea.net/legal.*

data protection legislation, thus falling within the scope of Article 6.1.e) of the GDPR; and **(iii)** whenever relating to internal regulations that do not involve criminal or administrative offences, the only viable grounds for legitimacy would be legitimate interest in accordance with article 6.1.f) of the GDPR. In such cases, your personal data will be processed with the utmost confidentiality and always in accordance with the GDPR and any other applicable data protection law.

In addition, the processing of personal third party data and information becomes justified under Article 6(1)(f) of the GDPR, which attributes a legitimate interest to FSP in carrying out investigations into activities in breach of the national legislative framework.

Furthermore, in case of receiving special categories of personal data from complainants or data subjects, the legitimate basis for processing stems from Article 6(1)(e) of the GDPR (public interest), and the exception to the prohibition on processing special categories of personal data set out in Article 9(2)(g) of the GDPR (essential public interest).

3. Categories of personal data processed and their source of origin

The Controller may process personal data containing the following types of information in any communications managed through the CII:

- Identifying data, such as name and surname, contact details and data relating to employee status, such as position or employee number, of both the person subject to the report and the person reporting.
- Relationship with Alsea Europe or other affected third parties.
- Data relating to the non-compliance reported or the communication made.
- Documentation that can provide evidence of the facts subject to the report.

The data that the Controller may process within the scope of CII operations derives from the following sources:

(i) Data provided by respondents via the CII.
(ii) Data generated as a consequence of the development, processing and maintenance of the relationship established between the informant and the Data Controller.
(iii) Personal data (additional information) provided by Alsea Europe group companies.
(iv) Data from third parties or publicly available sources.

4. Communication of your personal data

Your personal data may be disclosed to various recipients for the purpose of taking corrective actions within Alsea Europe or for processing the resulting disciplinary or criminal proceedings.

Within this scope, the Controller may communicate them (i) to the State Security and Investigative Forces, Public Administration entities with jurisdiction over the reported actions, Courts of Justice and other jurisdictional bodies, in the cases provided for in the Law and for the purposes defined therein; and (ii) to companies in the Alsea Europe group.

The legal basis for the communication of your data to the independent entities indicated in the previous paragraph will depend on the nature of the reported event. For this purpose, should the complaint involve possible breaches of laws or regulations, the legal basis for the communication of your personal data might derive from compliance with a legal obligation (Article 6(1)(c) of the GDPR) or a public interest (Article 6(1)(e) of the GDPR). Furthermore, should the complaint stem from non-compliance with internal rules that do not involve legal or regulatory breaches, the basis for legitimacy might arise from a legitimate self-interest (Article 6(1)(f) of the GDPR), provided that such interests do not override the rights and interests of the data subjects.

Likewise, other service providers may have access to the personal data under the responsibility of FSP in their capacities as data processors (consultants and external collaborators who provide support to the management or, where appropriate, investigation of the communications received through the CII and the service provider that runs the CII platform), with which FSP signs appropriate data processing contracts (in compliance with article 28 GDPR).

There will be no international transfers of your personal data to third countries or international organisations.

5. Duration of data processing

Your data will be kept for the time necessary for the investigation of the reported facts, bearing in mind that:

- Communications filed without action: when the communication does not comply with the formal requirements, concerns a doubt, query or complaint without involving an infringement, is manifestly irrelevant or demonstrates no indication of involving infringements, all data will be deleted from the system.
- Communication accepted for investigation: your personal data may be kept by the SII for the minimum period necessary to assess the launching of an investigation based on the facts reported. Should the information provided, or part of it, prove inaccurate, this will then be deleted immediately that this becomes apparent unless the aforementioned inaccuracy might constitute a criminal offence. In such cases, the information would be retained for as long as necessary and throughout the resulting legal proceedings.
- In any case, should no investigative action be initiated within three months of receipt of the report, the report shall then be deleted, unless (i) the purpose of its retention is to provide evidence of irregularities in the operation of the reporting system; (ii) it is necessary to process the personal data for a longer period in order to continue the investigation and/or for reasons of providing evidence the functioning of the IMS and/or because the decision was taken to initiate disciplinary and/or judicial proceedings against the person involved, the person who made the communication or a third party; in which case the data may be retained for the time required by the applicable legislation and thereafter, duly blocked, during the periods of limitation stipulated in the applicable legal requirements and any liabilities then arising from the data processing.

  However, when personal data, including special categories of data, are obtained in the course of the investigation and are not necessary for the purposes of knowledge and investigation of the facts, they shall be immediately deleted from the SII without any processing being carried out.

6. Rights

Data subjects, under the conditions established in the applicable regulations, hold the right to request access to their personal data, its rectification (if inaccurate), its deletion, limitation of processing or opposition, or to request the right to data portability (where applicable), as well as to not be subject to decisions based solely on the automated processing of their data (where applicable) by sending a written communication to the registered office of FSP as parent company of the group headquartered at Camino de la Zarzuela, 1 - 28023 Madrid, or to the e-mail address of the Data Protection Delegate of Alsea Europe specifically provided for this purpose: dpd@alsea.net.

Data subjects also hold the right to lodge complaints with the competent data protection authority in each case.

7. Security measures

With the aim of safeguarding the security of your personal data, the Data Controller undertakes to maintain the security and confidentiality of the data provided and, specifically, of the data of users who submit communications and reports through the CII and preventing access to those who caused the communication due to the alleged infringement within the organisation. To this end, the Data Controller has adopted the legally required levels of security for the protection of personal data and has deployed the technical means at its disposal to prevent the loss, misuse, alteration, unauthorised access and theft of the same even though absolute security does not exist.

Likewise, the Data Controller hereby informs that all staff, regardless of the processing stage in which they engage, are committed to processing your personal data with the utmost care and confidentiality.

8. Privacy policy update

The Data Controller may modify its Privacy Policy in accordance with the legislation applicable at any given moment in time. For this reason, it is advisable to read the Policy every time you access the website and/or carry out any procedure with our organisation.

ANNEX II. External information channels

1. In Spain:

Without prejudice to the preferential nature of Alsea Europe's CII, its Reporting Persons, provided that the information cannot be dealt with effectively by Alsea Europe or when perceiving a potential risk of retaliation, may report, including anonymously, the breaches regulated under paragraph 5.2 (i) of the Policy through the External Reporting Channel to:

a) The Independent Authority for the Protection of the Informant (A.A.I.), when the infringement reported affects or produces its effects in the territorial scope of more than one Autonomous Community.

b) The Independent Authority for the Protection of the Informant (A.A.I.) of the Autonomous Communities, when the infringement reported is limited to the territorial scope of the corresponding Autonomous Community.

In addition, they may report these infringements to, among other authorities, the following:

a) On labour conditions and workplace health and safety:

   (i) The Labour and Social Security Inspectorate for matters within its competence (labour, occupational health and safety, social security, employment, etc.). For these purposes, the actions and omissions of the responsible parties (natural or legal persons and joint owners) are considered social offences and are classified and sanctioned according to the civil regulations.

   (ii) ITSS Mailbox. The Ministry of Labour and Social Economy, through the State Agency of the Labour and Social Security Inspectorate, has made the "ITSS mailbox" available to all citizens for the reporting (not formal complaints) of certain types of labour irregularities that they may encounter. In this case, the reporter does not have to provide any personal data and the mailbox will only collect information on the alleged irregularities of which he/she is aware.

b) On data protection:

   (i) Through the different channels established on the AEPD's website: https://sedeagpd.gob.es/sede-electronica-web/

c) On consumer protection:

   (i) Through the local Municipal Consumer Information Office or the Directorate-General for Consumer Affairs of the respective Autonomous Community https://www.consumo.gob.es/es/consumo/reclamaciones

d) On tax matters:

   (i) The Tax Agency's Complaints Channel may be used to officially report facts or situations that may constitute tax infringements or smuggling or matters that may be of importance for the collection of taxation https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html.

2. In Belgium

Belgian law designates the Federal Ombudsman (Federal Mediator) as the coordinating body in charge of receiving communications and forwarding them to the specific subject or sector body responsible (such as the Financial Services and Markets Authority, the National Bank of Belgium and the Data Protection Authority).

3. In France

The French law enables Whistleblowers to submit external complaints to:

a) The competent state institutions designated by the Council of State.

b) Decrees of the Council of State.

c) The French institution called the "Defender of Rights", which will in turn forward the report to the competent state institution.

d) The Judicial Authorities.

e) EU institutions, bodies or organisations competent for receiving information on breaches of EU law.

f) Federal mediators.

4. In the Netherlands

The competent external authorities in accordance with Dutch law are:

a) The Consumer and Markets Authority;

b) the Netherlands Authority for the Financial Markets;

c) The Dutch Data Protection Authority;

d) De Nederlandsche Bank NV;

e) The Health and Youth Inspectorate;

f) The Whistleblowers' Chamber;

g) The Dutch Health Authority;

h) Nuclear Safety and Radiation Protection Authority, and

i) organisations and administrative bodies, or parts thereof, designated by order in council or ministerial regulation with responsibilities or powers in one of the areas referred to in the first paragraph of Article 2 of the Directive.

5. In Luxembourg

Article 18 of the Luxembourg legislation lists the competent authorities which Informants may address. These are:

a) The Financial Sector Supervisory Commission.

b) The Commissariat aux assurances.

c) The Competition Authority.

d) The Administration de l'enregistrement, des domaines et de la TVA.

e) The Labour and Mines Inspectorate.

f) The National Data Protection Commission.

g) The Centre for Equal Treatment.

h) The Ombudsman within the framework of its mission for external controls over incidences of deprivation of liberty.

i) Ombudsman fir Kanner a Jugendlecher.

j) The Institut luxembourgeois de régulation.

k) The Autorité luxembourgeoise indépendante de l'audiovisuel.

l) The Ordre des avocats du Barreau de Luxembourg and l'Ordre des avocats du Barreau de Diekirch.

m) The Notary Association.

n) The Medical Association.

o) Nature and Forest Management Authority.

p) Water Management Authority.

q) The Air Navigation Administration.

r) The National Consumer Ombudsman Service.

s) The Ordre des architectes et des ingénieurs-conseils.

t) The Ordre des experts-comptables.

u) The Institut des réviseurs d'entreprises.

v) The Administration des contributions directes.

6. In Portugal

External complaints shall be lodged with the authorities which, according to their powers and functions, should or may have knowledge of the matter subject to complaint, including:

a) The Public Prosecutor's Office.

b) Criminal police forces.

c) The Bank of Portugal.

d) Independent administrative authorities.

e) Public institutes.

f) The General Inspectorates and similar entities and other central services of the direct State Administration with administrative autonomy.

g) Local authorities.

h) Public partnerships.

7. At the European level:

The external channels to which Informants may turn include:

On data protection:

a) Through the portal of the European Data Protection Committee (ECDC), for certain issues https://edpb.europa.eu/about-edpb/more-about-edpb/contact-us_es

b) Through the portal of the European Data Protection Supervisor (EDPS) https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en

On consumer protection:

a) Through the European platform http://ec.europa.eu/consumers/odr/.