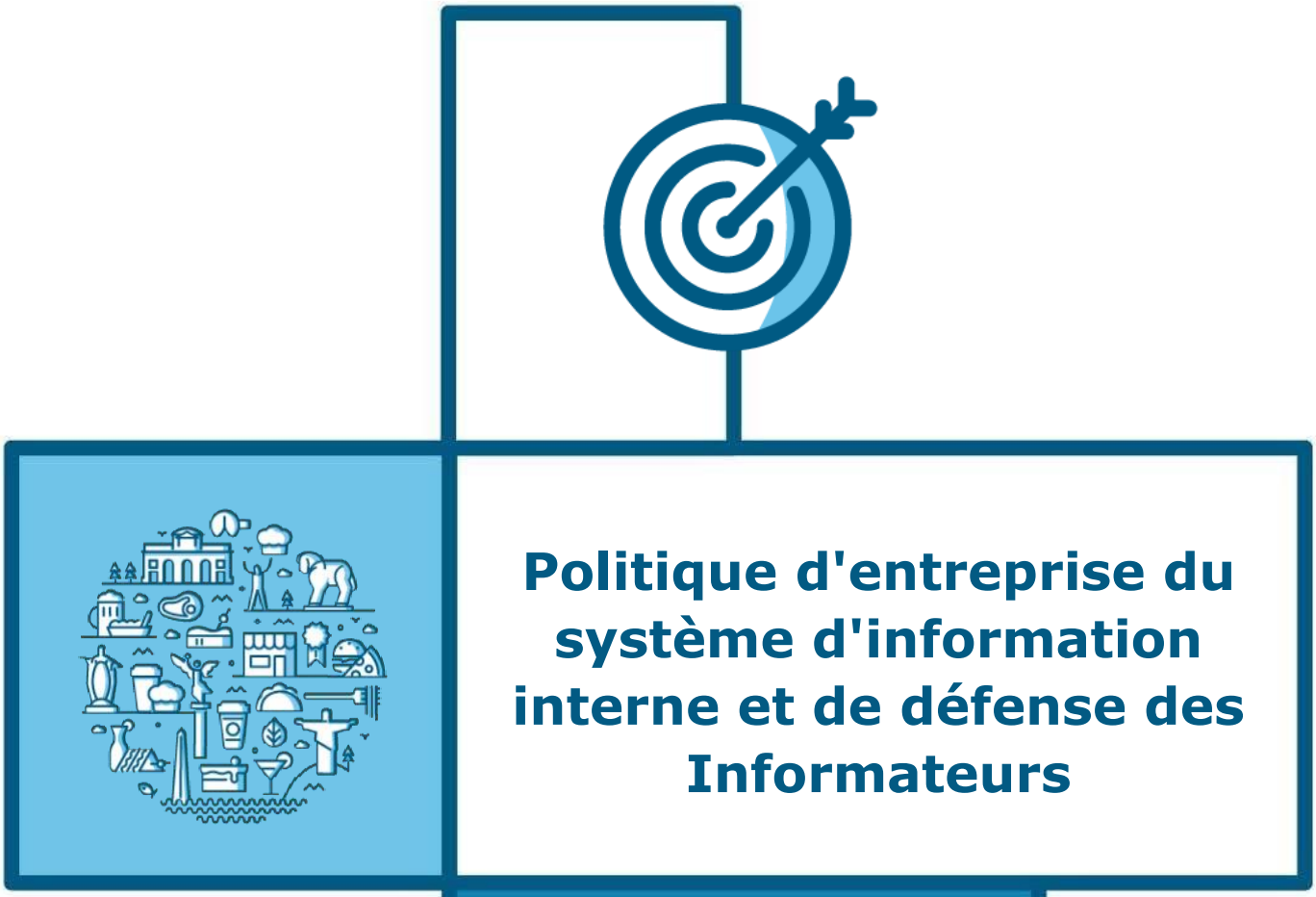
Alsea



Politique d'entreprise du système d'information interne et de défense des Informateurs

POL-CUMP-EUR-022

Description générale du document	
Titre du document :	Politique d'entreprise du système d'information interne et de défense des Informateurs
Domaine :	Conformité
Macro-processus :	Cadre réglementaire - Politiques générales
Processus :	Conformité et gestion des risques
Sous-processus :	Conformité
Champ d'application :	L'Europe
Version :	01
Date de la dernière version :	07/06/2024
Préparé par :	Responsable de la conformité Alsea Europe
Révisé par :	Comité de conformité Alsea Europe
Approuvé par :	Conseil d'administration d'Alsea Europe
Vérifié pour Contrôle interne :	Comité de conformité Alsea Europe

Registre des versions								
Version	1	2	3	4	5	6	7	8
Date	07/06/2024							

Contenu

1. Objectif

Comme établi dans le Code d'éthique et de conduite professionnelle d'Alsea Europe[1] (ci-après, indistinctement, « ***Alsea Europe*** », la « ***Société*** » ou le « ***Groupe*** »), chacun des salariés[2] travaillant à Alsea Europe et les tiers avec lesquels Alsea Europe a une relation commerciale ou professionnelle doivent se comporter avec intégrité et exercer leurs activités conformément à la loi et aux règlements internes d'Alsea Europe.

De même, il est du devoir des personnes ou entités susmentionnées, dans le cadre de la prévention et de la détection des comportements irréguliers ou illégaux, de signaler toute allégation d'irrégularité ou d'acte contraire à la loi ou aux règles internes dont elles ont connaissance.

À cette fin, Alsea Europe a mis en place un système d'information interne (ci-après « **SII »**) conformément aux exigences énoncées dans les lois applicables aux sociétés composant Alsea Europe transposant la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union (ci-après « ***directive 2019/1937*** »)[3] .

Cette Politique d'entreprise en matière de SII et de défense des Informateurs (ci-après, la « ***Politique*** »), approuvée par le Conseil d'Administration de FOOD SERVICE PROJECT, S.A. (ci-après, « ***FSP*** »), d'une part, démontre l'engagement ferme d'Alsea Europe à assumer les bonnes pratiques de gouvernance d'entreprise et le développement d'une culture de conformité éthique et réglementaire, qui promeut et renforce, parmi ses parties prenantes - tant internes qu'externes - une culture adéquate d'information et de communication comme un mécanisme qui aide ALSEA EUROPE à prévenir et détecter les conduites irrégulières et, de cette façon, à être capable de réagir à celles-ci. D'autre part, elle établit les règles et les principes généraux qui régissent le SII constitué de l'ensemble des ressources humaines, matérielles et économiques visant à assurer : (i) la protection des Informateurs qui signalent des infractions relevant du champ d'application de la présente Politique, (ii) ainsi que leur traitement approprié et efficace.

2. Système d'information interne (SII)

Le SII d'Alsea Europe : (i) a un responsable ; (ii) intègre les différents canaux d'information internes mis en place dans la société ; (iii) comprend une Procédure spécifique de gestion des informations reçues (ci-après, la « ***Procédure*** ») qui, afin de promouvoir une culture de l'information interne, garantit la protection de l'Informateur et a été approuvée par le Conseil d'administration de FSP ; et (iv) est indépendant des systèmes d'information internes d'autres entités et organismes.

---

[1] Aux fins du présent document, le groupe de sociétés « Alsea Europe » comprend à la fois FOOD SERVICE PROJECT, S.A. (FSP) et les sociétés - actuelles ou futures - dont FSP détient, directement ou indirectement, la majorité des actions, des participations ou des droits de vote, ou dont elle a nommé ou a le pouvoir de nommer la majorité des membres de l'organe de direction ou d'administration, de telle sorte qu'elle contrôle effectivement la société.

[2] Aux fins de la présente politique, les employés sont définis comme tous les employés qui fournissent des services aux sociétés qui composent Alsea Europe.

[3] Aux fins de la présente politique, la législation applicable aux sociétés composant Alsea Europe en la matière est : (i) Belgique : La loi du 28 novembre 2022 relative à la protection des lanceurs d'alerte en cas de violation du droit national ou du droit de l'Union européenne établis au sein d'une personne morale du secteur privé, entrée en vigueur le 15 février 2023 ; (ii) France : La loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte ; (iii) Pays-Bas : Loi néerlandaise transposant partiellement la directive entrée en vigueur le 18 février 2023 ; (iv) Luxembourg : Loi du 16 mai 2023 transposant la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union ; (v) Portugal : Loi n° 93/2021 du 20 décembre 2021 ; et (vi) Espagne : Loi 2/2023 du 20 février réglementant la protection des personnes qui signalent des infractions réglementaires et la lutte contre la corruption.

3. Documents connexes

Code	Nom du document
POL-CUMP-EUR-001	Code d'éthique et de conduite professionnelle
POL-CUMP-EUR-002	Politique anticorruption de l'entreprise
POL-CUMP-EUR-003	Politique de l'entreprise Conflit d'intérêts
POL-RH-EUR-001	Politique de prévention des risques professionnels
POL-AJ-EUR-001	Politique de protection des données de l'entreprise
POL-CUM-EUR-003	Politique en matière de cadeaux et d'invitations
POL-CUMP-EUR-005	Politique de gestion des risques de l'entreprise
POL-CUMP-EUR-006	Politique de conformité de l'entreprise
PRO-CUMP-EUR-009	Procédure de gestion des informations reçues

4. Responsable du système d'information interne (RSII) et gestionnaire du canal d'information interne (CII)

Le Conseil d'administration de FSP a désigné le Comité de conformité (ci-après, le « ***RSII*** ») comme l'organe responsable de la supervision et de la gestion du SII, qui, en tant qu'organe collégial, désignera parmi ses membres un responsable du Canal d'information interne (ci-après, le « ***Gestionnaire du SII*** »).

Le suivi, la supervision et l'interprétation de la présente Politique et de la Procédure, sans préjudice des compétences réservées au conseil d'administration de FSP, relèvent de la responsabilité du RSII. En outre, il est chargé d'en assurer le respect et, le moment venu, l'interprétation et la mise à jour lorsque cela est approprié ou en cas de changements organisationnels, de structure de contrôle, d'activités exercées et/ou de changements législatifs ou jurisprudentiels.

Nonobstant ce qui précède, le gestionnaire du SII, dans le cadre de ses fonctions et sans préjudice des pouvoirs du RSII, peut élaborer les règles de mise en œuvre ou les guides relatifs à la présente Politique et Procédure qu'il juge nécessaires pour assurer le bon fonctionnement du SII.

5. Champ d'application

5.1. Champ d'application subjectif

Alsea Europe a mis en place son SII comme un canal de communication public accessible à tous ceux:

(i) qui travaillent ou ont travaillé dans les différentes entreprises qui composent Alsea Europe (par exemple : cadres, employés, stagiaires, etc.) ; ou
(ii) qui sont ou ont été membres de son organe administratif ou exécutif ; ou
(iii) qui interagissent ou ont interagi, dans tout ou partie du processus commercial, avec ou sans implication dans la réalisation des objectifs et des résultats d'Alsea Europe ; ou
(iv) les parties externes qui ont eu, ont ou peuvent avoir une relation directe et un intérêt commercial et/ou professionnel légitime et raisonnable (actionnaire, client, fournisseur et ses employés, franchisés et leurs employés, bénévoles, etc.)

Toutes ces personnes sont ci-après dénommées collectivement les « ***Informateurs*** ».

5.2. Qu'est-ce qui doit être signalé par le biais du système d'information interne (SII) ?

Le SSI n'est pas une boîte à plaintes ou à suggestions, mais un système qui vise à : (i) dissuader les contrevenants potentiels ; (ii) garantir que toutes les actions potentiellement irrégulières peuvent être signalées et, si nécessaire, faire l'objet d'une enquête en bonne et due forme ; (iii) dissiper les doutes ; et (iv) mettre en place les mesures nécessaires pour assurer la protection des personnes qui collaborent à la notification et à la clarification d'éventuelles infractions.

Compte tenu de ce qui précède, les Informateurs peuvent, par l'intermédiaire du SII, signaler des actions ou des omissions constituant des infractions ou des non-conformités survenant dans le cadre du travail ou de la profession et liées à l'une des sociétés qui composent le groupe dans les domaines suivants :

(i) Infractions aux lois européennes et locales applicables à Alsea Europe :

a) Infractions au droit de l'Union européenne (UE), au cas où ces infractions :

- ont un impact sur des questions telles que : les marchés publics ; les services, produits et marchés financiers, et la prévention du blanchiment d'argent et du financement du terrorisme ; la sécurité des produits ; la sécurité des transports ; la protection de l'environnement ; la protection des consommateurs ; et la protection de la vie privée et des données à caractère personnel, ainsi que des réseaux et des systèmes d'information ;
- constituent une fraude ou une activité illégale portant atteinte aux intérêts de l'Union européenne ; ou
- affectent le marché intérieur[4], y compris les infractions aux règles de concurrence de l'UE et les aides accordées par les États membres, ainsi que les infractions concernant le marché intérieur liées à des actes contraires aux règles de l'impôt sur les sociétés ou à des pratiques visant à obtenir un avantage fiscal qui irait à l'encontre de l'objet ou de la finalité de la législation relative à l'impôt sur les sociétés.

b) les infractions pénales ; et

c) Infractions administratives mineures, graves ou très graves.

En tout état de cause, il s'agit de toutes les infractions relatives au harcèlement moral ou sexuel, aux infractions relatives au travail et à la santé et la sécurité au travail, ainsi qu'aux infractions administratives entraînant un préjudice financier pour le Trésor public et la sécurité sociale.

Les infractions pénales et administratives susmentionnées sont régies par les dispositions des lois locales applicables à Alsea Europe.

(ii) Autres irrégularités en matière de conformité qui ne sont pas incluses dans ce champ d'application (i), en particulier celles liées au non-respect du code d'éthique et de conduite professionnelle d'Alsea Europe ou de toute autre règle interne d'Alsea Europe (par exemple, politiques, protocoles, etc.).

(iii) Consultations sur la conformité réglementaire.

Toutes les communications sur les infractions et les demandes de renseignements soumises par l'intermédiaire du SII seront reçues par le Gestionnaire du CII. Le Gestionnaire du CII sera chargé de les gérer conformément à la procédure de gestion des informations reçues.

Ainsi, avec la mise en place du canal d'information interne (ci-après, le « ***CII*** »), les canaux suivants sont intégrés au SII et, par conséquent, ne sont plus en vigueur :

a) le canal des Informateurs, en désactivant l'adresse électronique canaletico@alsea.net

[4] *Le marché intérieur comporte un espace sans frontières intérieures dans lequel la libre circulation des marchandises, des personnes, des services et des capitaux est assurée selon les dispositions des traités.*

b) Le canal de protection des données dpd@alsea.net pour les violations de la protection des données et les infractions.

5.3. Quelles sont les communications exclues du système d'information interne (SII) ?

Comme indiqué ci-dessus, il ne s'agit pas d'une boîte aux lettres pour les plaintes ou les suggestions, et doit être utilisé de manière responsable et dans le cadre des objectifs pour lesquels il est prévu, et le suivant ne doit donc pas être communiqué par l'intermédiaire du SII:

a) Informations générales relatives à Alsea Europe.
b) Plaintes de nature commerciale ou de facturation.
c) Questions pour lesquelles il existe un canal spécifique (service à la clientèle, exercice des droits en matière de RGPD, etc.).
d) Doutes, questions, réclamations et plaintes d'ordre professionnel ou salarial.
e) Plaintes concernant les installations ou leur état.

À cette fin, les canaux ordinaires resteront disponibles pour les communications, les demandes, les requêtes ou les observations relatives, entre autres, à ce qui suit :

- A l'exercice des droits en matière de RGPD[5] .
- Service à la clientèle.
- Communication externe.
- Demande de factures.
- Talents et sélection.
- Canaux d'emploi.
- Candidats franchisés.

Les informations communiquées par ces canaux continueront d'être gérées par les canaux et moyens existants et conformément à leurs procédures spécifiques.

6. Types et moyens de communication

6.1. Types de communication

6.1.1. Consultations

L'objectif des consultations est de suggérer des changements ou des améliorations ou, le cas échéant, de soulever des questions concernant le code d'éthique et de conduite professionnelle d'Alsea Europe, toute autre règle interne d'Alsea Europe ou la loi applicable, ou dont l'application est douteuse, lorsqu'il s'agit de règles de conformité et/ou de prévention de la criminalité.

Toute préoccupation relative à une action ou à un comportement susceptible d'avoir un impact sur les règles de conformité et/ou de prévention de la criminalité doit également faire l'objet d'une demande d'information.

6.1.2. Plaintes

L'objectif de la dénonciation est de signaler les risques ou les violations des règles applicables, qu'elles soient internes ou légales, en particulier pour la dénonciation de la commission présumée de délits, comme indiqué à la section 5.2 de la présente Politique. Ce type de communication peut être utilisé pour signaler des infractions ou des violations déjà commises ou prévisibles sur la base d'indices raisonnables, voire l'existence de risques non détectés qui pourraient faciliter leur commission.

[5] *Les droits d'accès, de rectification, d'annulation, d'opposition, de portabilité, de suppression et de limitation en matière de protection des données*.

6.2. Moyens de communication

Les communications peuvent être effectuées par les canaux suivants :

a) En priorité, par le biais du lien qu'Alsea Europe met à la disposition des Informateurs sur le site web de l'entreprise.

b) Par courrier ordinaire à Camino de la Zarzuela, 1, Madrid (28023) Espagne, à l'attention du Gestionnaire du CII.

c) Sur demande de la partie déclarante, en personne, soit par la remise en main propre de la plainte écrite, soit verbalement, à l'adresse Camino de la Zarzuela, 1, Madrid (28023) Espagne, au Gestionnaire du CII, qui sera chargé de déterminer les conditions dans lesquelles la remise aura lieu afin de préserver la confidentialité ; et, dans le cas d'une communication verbale, de la recueillir par écrit, accompagnée de la signature de l'Informateur. Une réunion en distanciel avec le Gestionnaire du CII peut également être demandée.

d) Applicable exclusivement pour les cas de harcèlement moral ou sexuel, la plainte peut être soumise, au choix du travailleur, aux organes prévus à cet effet par la Procédure de prévention et de traitement des situations de harcèlement moral ou sexuel applicable au Groupe au niveau local (à titre purement exemplaire, le Comité d'instruction pour le traitement des situations de harcèlement, le médecin affecté au service de prévention, les représentants légaux des travailleurs sur le lieu de travail).

Toutes les communications, quel que soit le canal par lequel elles sont effectuées, doivent être envoyées au Gestionnaire du CII, qui sera chargé de les enregistrer dans le CII en vue de leur gestion ultérieure conformément aux dispositions de la présente Politique.

7. Contenu des communications

7.1. Consultations

La consultation doit préciser les aspects spécifiques du code d'éthique et de conduite professionnelle d'Alsea Europe, de toute autre règle interne ou du droit applicable pour lesquels se posent des questions d'interprétation et/ou d'application, de changements ou d'améliorations.

7.2. Plaintes

Pour que la plainte soit recevable, les points suivants doivent, dans la mesure du possible, être clairement indiqués :

- Relation de l'Informateur avec Alsea Europe : collaborateur, fournisseur, franchisé, client, etc.
- Une description claire et détaillée des faits ou du comportement potentiellement irrégulier, avec une attention particulière :
  - ✓ Date ou période des événements.
  - ✓ Moyens utilisés pour commettre le comportement illicite possible/ présumé.
  - ✓ S'il y a d'autres personnes qui peuvent fournir des informations supplémentaires ou corroborer leur témoignage.
  - ✓ Domaine d'activité ou entreprise concerné(e).
- Dans la mesure du possible, l'identification des personnes présumées responsables de l'irrégularité ou, à défaut, l'indication des données permettant de connaître l'identité de la (des) personne(s) présumée(s) responsable(s).
- S'ils sont disponibles, fournir des documents ou des preuves en rapport avec les faits reprochés.

- Déclaration de l'Informateur selon laquelle il a lu l'avis relatif à la protection des données et a été informé du traitement de ses données à caractère personnel conformément aux dispositions de l'**annexe I**.

Les Informateurs sont avertis qu'ils doivent s'efforcer de fournir les informations requises pour rapporter un fait donné et éviter de fournir des données excessives ou inutiles (par exemple, des documents obtenus de manière irrégulière ou appartenant à un tiers, des documents qui ne sont pas directement liés aux faits rapportés, etc.) Si le rapport ne contient pas les informations nécessaires à l'ouverture de l'enquête, des informations ou des documents supplémentaires ou complémentaires peuvent être demandés à l'Informateur pour qu'il soit admis au traitement.

Les plaintes relatives à des informations exclues du champ d'application du SII ne sont pas recevables.

7.3. Informations interdites

Toutes les communications contraires au système juridique sont exclues du SII, y compris celles qui touchent aux informations classifiées et au secret professionnel, par exemple celles de la profession juridique et la confidentialité des forces et des corps de sécurité dans le cadre de leurs actions.

8. Procédure de gestion des informations reçues

Toutes les demandes et plaintes reçues seront gérées et traitées conformément aux règlements applicables et aux dispositions de la Procédure.

Étant donné que toutes les violations de la conformité sont soumises au SII et seront donc traitées conformément aux dispositions de la Procédure, la version actuelle du protocole de fonctionnement et de gestion du canal de traitement des plaintes d'Alsea Europe sera remplacée et supplantée par la version actuelle du protocole de fonctionnement et de gestion du canal de traitement des plaintes d'Alsea Europe.

En outre, la Procédure susmentionnée inclura les règles établies en matière de harcèlement moral et sexuel qui peuvent être incluses dans les procédures de prévention et de traitement des situations de harcèlement moral ou sexuel qui peuvent être applicables au groupe au niveau local.

8.1. Principes

La Procédure décrite dans la présente Politique repose sur les principes de confiance, de proportionnalité, d'impartialité, de véracité et de confidentialité, sur les droits à l'honneur, à la présomption d'innocence, à la défense, à la non-incrimination et à la protection effective des droits de l'Informateur et de la personne faisant l'objet de l'enquête, ainsi que sur la protection de l'Informateur contre d'éventuelles représailles.

La Procédure ne peut en aucun cas violer les règles régissant les procédures pénales, y compris les procédures d'enquête.

8.2. Gestion des informations reçues

Toutes les informations communiquées par l'intermédiaire du SII, quel que soit le canal ou le support utilisé, seront reçues par le Gestionnaire du CII.

Le Gestionnaire du CII est chargé de décider : (a) de l'admission et du traitement ou de l'archivage des informations reçues ; ou (b) du renvoi au responsable compétent pour traitement ou archivage, dans les deux cas conformément à la Procédure.

Les rapports de harcèlement (moral ou sexuel) sont reçus par le Gestionnaire du CII. En cas d'infraction pénale, le rapport sera traité par le Gestionnaire du CII et, en cas d'infraction administrative, par l'organe qui peut être établi à cet égard par les procédures de prévention et de traitement des situations de harcèlement moral ou sexuel applicables au groupe au niveau local (par exemple: le comité d'enquête sur les situations de harcèlement (CITSA)). En tout état de cause, la procédure applicable à ces informations est la Procédure.

Dans les sept (7) jours civils suivant la réception de l'information, le Gestionnaire du CII envoie à l'Informateur un accusé de réception.

Le Gestionnaire du CII, après avoir envoyé l'accusé de réception, décide de l'admission, de l'irrecevabilité ou du renvoi de l'information au responsable compétent en fonction du sujet traité. En cas d'admission, la ou les parties enquêtées sont notifiées conformément aux dispositions de la Procédure. En aucun cas l'identité de l'Informateur ne sera communiquée à la personne ou aux personnes faisant l'objet de l'enquête, ni ne leur donnera accès à la communication/plainte. En tout état de cause, l'Informateur sera informé de l'admission ou de la clôture de la communication.

L'enquête relève de la responsabilité du Gestionnaire du CII qui, en fonction du sujet de la communication, peut la déléguer en tout ou en partie à d'autres membres de l'organisation et/ou à des conseillers externes, comme c'est le cas pour les enquêtes portant sur des infractions pénales graves, qui peuvent être confiées à des conseillers externes spécialisés.

La résolution du dossier d'enquête ne peut excéder trois (3) mois à compter de l'accusé de réception de la communication ou, si aucun accusé de réception n'a été envoyé à l'Informateur, trois (3) mois à compter de l'expiration du délai de sept (7) jours suivant la communication, sauf dans les cas particulièrement complexes où l'enquête peut être prolongée d'un maximum de trois (3) mois supplémentaires.

Ces délais sont réduits dans les cas de harcèlement moral ou sexuel, afin de respecter les délais qui peuvent être fixés à cet égard dans les procédures de prévention et de traitement des situations de harcèlement moral ou sexuel applicables au groupe au niveau local.

Une fois l'enquête terminée, l'organisme qui l'a menée publiera et, si nécessaire, partagera avec le Gestionnaire du CII un rapport final reprenant les conclusions de l'enquête.

En cas de harcèlement moral ou sexuel, une fois l'enquête menée à bien par l'organe compétent et conformément à la Procédure, l'organe compétent adopte les mesures appropriées conformément à la procédure de prévention et de traitement des situations de harcèlement moral et sexuel applicable au groupe au niveau local.

Si les conclusions du rapport final de l'enquête indiquent qu'il s'agit d'un acte présumé délictueux dont la responsabilité pénale du groupe peut être directement engagée, le rapport final est transmis au RSII, qui décide des mesures disciplinaires et/ou judiciaires à adopter, ainsi que de l'éventuelle communication aux autorités judiciaires compétentes et/ou au ministère public ou au ministère public européen, si les faits portent atteinte aux intérêts financiers de l'Union européenne.

Le SII tient un registre des informations reçues, en attribuant un code d'identification à chaque dossier. Ce registre n'est pas public.

8.3. Droits et garanties des Informateurs

Les auteurs de rapports qui signalent des violations telles que décrites au point 5.2 de la présente Politique bénéficient des droits et garanties suivants :

a) Décider si la communication est effectuée de manière anonyme ou non. Dans le cas où l'Informateur opte pour la modalité non anonyme, la confidentialité de son identité sera garantie tant par le RSII que par le Gestionnaire du CII et les personnes qui, le cas échéant, interviennent dans le traitement de l'information.

b) Formuler la communication par écrit et/ou verbalement. Le CII autorisé dispose d'un mécanisme qui empêche son identification par des tiers.

c) Être informé de l'état d'avancement du traitement et de la suite donnée à votre communication. Par conséquent, vous pouvez choisir de recevoir des notifications ou des communications relatives à l'admission et au traitement des informations ou renoncer expressément à ce droit. En cas de choix de recevoir des notifications, l'Informateur peut choisir de maintenir ou non un dialogue anonyme.

d) Comparaître devant le Gestionnaire du CII de sa propre initiative ou à sa demande, avec l'assistance d'un avocat si nécessaire.

e) Exercer les droits en matière de protection des données personnelles.

8.3.1. Droit à la confidentialité

Le SII garantit la confidentialité de l'identité de l'Informateur et de tout tiers mentionné dans la communication, ainsi que des actions menées dans le cadre de sa gestion et de son traitement. Il garantit également la protection des données, en empêchant l'accès au personnel non autorisé.

De même, lorsqu'une communication relevant du SII, qu'il s'agisse d'une requête ou d'une plainte, est envoyée par un canal autre que le CII ou est soumise à d'autres employés ou représentants que le RSII ou le Gestionnaire du CII, ceux-ci sont tenus d'en garantir la confidentialité et de la signaler immédiatement au Gestionnaire du CII pour qu'elle soit traitée. Le non-respect de cette obligation par l'employé ou le représentant sera considéré comme une violation très grave de la présente Politique et, par conséquent, comme une violation de leurs obligations professionnelles ou contractuelles.

L'identité de la personne déclarante ne peut être divulguée à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente que dans le cadre d'une enquête pénale, disciplinaire ou prud'homale. Les divulgations effectuées en vertu du présent paragraphe sont soumises aux garanties prévues par la réglementation applicable. En particulier, l'Informateur est informé avant que son identité ne soit révélée, sauf si cette communication risque de compromettre l'enquête ou la procédure judiciaire.

8.3.2. Droit à l'anonymat

L'Informateur peut décider s'il souhaite faire son rapport de manière anonyme et, par conséquent, le SII garantit un accès anonyme à la CII, tant pour déposer la plainte initiale que pour communiquer avec Alsea Europe chaque fois qu'il le juge nécessaire dans le cadre du dossier ouvert à la suite de la plainte.

8.3.3.Interdiction de représailles

Il est strictement interdit d'adopter toute forme de représailles, de discrimination et de pénalisation sur la base de plaintes déposées contre un Informateur qui, de bonne foi et avec des motifs raisonnables à l'appui, porte à l'attention d'Alsea Europe, par l'intermédiaire du SII, la commission présumée d'un comportement relevant du champ d'application du SII. Cette garantie s'étend également à toute personne participant à l'enquête (par exemple, les témoins, la partie lésée, etc.), à condition que leur intervention soit faite de bonne foi.

Par représailles, on entend toute action ou omission interdite par la loi ou qui, directement ou indirectement, entraîne un traitement défavorable pour la ou les personnes qui en sont victimes dans le cadre de leur travail ou de leur profession, uniquement en raison de leur statut d'Informateur ; à condition que cette action ou omission ait lieu pendant la phase d'enquête ou dans les deux (2) ans qui suivent son achèvement. Une exception est faite dans les cas où une telle action ou omission peut être objectivement justifiée par un objectif légitime et où les moyens utilisés pour atteindre cet objectif sont nécessaires et appropriés.

En cas de violation de cette garantie, celle-ci doit être signalée pour enquête et, si elle est confirmée, l'auteur des représailles peut faire l'objet d'une action disciplinaire.

Les personnes qui communiquent dans les cas suivants sont expressément exclues de la protection prévue au présent paragraphe :

a) Les informations ont déjà été communiquées précédemment par l'intermédiaire de la CII et ont été rejetées.
b) Les informations relatives à des allégations de conflits interpersonnels ou n'affectant que la personne déclarante et les personnes auxquelles la communication ou la divulgation se rapporte.
c) Les informations qui sont déjà pleinement accessibles au public ou qui constituent de simples ouï-dire.

d) Les informations relatives aux actions ou omissions non couvertes par la section 5.2 de la présente Politique.

Les personnes qui ont signalé de manière anonyme des informations sur les infractions visées au point 5.2 de la présente Politique, mais qui ont été identifiées par la suite et ne répondent pas aux critères d'exclusion susmentionnés, ont le droit d'être protégées contre les représailles.

8.3.4. Agir de bonne foi

Si l'enquête détermine que la communication est fausse et que l'Informateur l'a faite en connaissance de cause ou au mépris de la vérité, la responsabilité pénale ou civile et/ou les mesures disciplinaires appropriées peuvent être exigées, dans les conditions prévues par la législation en vigueur et le régime disciplinaire d'Alsea Europe, et les exigences de confidentialité peuvent également être levées.

L'utilisation du SII de mauvaise foi n'est pas une pratique acceptable et l'utilisation abusive de ce système fera l'objet de poursuites.

En ce sens, les Informateurs seront considérés comme étant de mauvaise foi lorsqu'ils :

- sont conscients de la fausseté des faits.
- agissent au mépris flagrant de la vérité.
- agissent avec l'intention de se venger et de nuire à la personne dénoncée ou à l'entreprise.
- agissent dans l'intention de porter atteinte à l'honneur ou à la réputation professionnelle ou commerciale de toute personne associée à Alsea Europe.

8.4. Droits de la personne faisant l'objet de l'enquête

La personne faisant l'objet d'une enquête a droit à la présomption d'innocence, à la défense et à l'accès au dossier d'enquête, ainsi qu'à la protection effective de ses droits. À cette fin, elle reçoit un bref exposé des faits sur lesquels porte l'enquête, a le droit de formuler toute allégation et de fournir les éléments de preuve qu'elle juge nécessaires à sa défense, et a accès au dossier d'enquête, bien qu'en aucun cas l'identité de l'Informateur ne soit communiquée à la personne faisant l'objet de l'enquête, et qu'elle n'ait pas non plus accès à la plainte. De même, la personne faisant l'objet de l'enquête peut être assistée d'un avocat.

La personne faisant l'objet de l'enquête a droit à la même confidentialité que celle établie pour les Informateurs, en préservant son identité et les faits et données figurant dans le dossier d'enquête.

8.5. Conflit d'intérêts

Si les informations communiquées par l'intermédiaire du SII concernent le RSII ou le Gestionnaire du CII et/ou toute autre personne susceptible d'intervenir dans sa gestion et son traitement, leur abstention et leur interdiction absolue d'intervenir dans le traitement (admission, enquête et résolution) de l'enquête telle qu'elle est développée dans la Procédure sont garanties.

9. Canaux externes

Le SII mis en place par Alsea Europe sera le canal privilégié pour signaler les actions ou omissions visées à la section 5.2 (i) de la présente Politique, à condition que le déclarant considère que la violation peut être traitée efficacement et qu'il n'y a pas de risque de représailles. L'**annexe II** de la présente Politique énumère, à titre d'exemple mais sans s'y limiter, certains canaux externes dans les pays où Alsea Europe exerce ses activités. Nonobstant ce qui précède, les employés d'Alsea Europe sont tenus de signaler par l'intermédiaire du SII toute violation des règles internes énoncées à la section 5.2(ii) lorsqu'elle ne constitue pas une violation des règles énoncées à la section 5.2(i).

9.1. Coopération avec les autorités

Alsea Europe, à condition que son droit de défense et le droit de ne pas s'auto-incriminer ne soient pas compromis, coopérera et/ou répondra avec la plus grande diligence aux demandes faites par les autorités administratives et judiciaires, le ministère public ou le ministère public européen en relation avec des actions liées à Alsea Europe ou pour toute autre raison. L'attention portée à ces exigences sera gérée par le Comité de conformité, qui devra en informer immédiatement le Conseil d'administration de FSP, à condition que les faits à l'origine de l'exigence puissent entraîner une responsabilité pénale directe pour le groupe.

10. Protection des données personnelles

Dans le cadre de la gestion du SII, les dispositions légales applicables en matière de protection des données à caractère personnel seront respectées ; à cet effet, les « Informations sur le traitement des données à caractère personnel » figurent à l'***annexe I***.

11. Non-conformité

Toute violation de cette Politique par les employés d'Alsea Europe sera analysée conformément aux procédures internes, aux réglementations légales et aux accords en vigueur et, le cas échéant, les mesures disciplinaires correspondantes seront appliquées au contrevenant, sans préjudice de toute autre responsabilité (pénale ou autre) que le contrevenant pourrait avoir encourue.

12. Diffusion et approbation

Cette Politique est accessible à tous les employés d'Alsea Europe, ainsi qu'aux tiers, grâce à sa publication sur le site Internet de l'entreprise.

Alsea Europe prendra les mesures nécessaires pour diffuser, former et informer tous ses employés sur le SII, ses principes, garanties et obligations, ainsi que son objectif.

Cette Politique a été approuvée par le conseil d'administration de FSP le 07 de Juin de 2024, avec effet à cette date.

ANNEXE I. Informations sur le traitement des données à caractère personnel

INFORMATIONS DE BASE SUR LA PROTECTION DES DONNEES (PREMIER NIVEAU)

Responsable du traitement : FOOD SERVICE PROJECT, S.A.

Finalité : gérer les informations traitées par l'intermédiaire du CII.

Droits : La personne concernée peut exercer, le cas échéant, ses droits d'accès, de rectification, d'effacement, d'opposition, de portabilité, de limitation, ainsi que le droit de ne pas faire l'objet de décisions individuelles automatisées, en écrivant à dpd@alsea.net ou à l'adresse postale Camino de la Zarzuela, 1. Madrid (Espagne). La personne concernée peut également introduire une réclamation auprès de l'autorité de contrôle compétente en matière de protection des données.

Informations complémentaires : La personne concernée peut consulter des informations complémentaires et détaillées en cliquant sur la « Politique de confidentialité » créée pour ce traitement spécifique.

POLITIQUE DE CONFIDENTIALITÉ ET INFORMATIONS SUPPLÉMENTAIRES SUR LA PROTECTION DES DONNÉES (DEUXIEME NIVEAU)

1. Responsable du traitement des données et coordonnées du délégué à la protection des données

Conformément à la réglementation sur la protection des données personnelles, FOOD SERVICE PROJECT, S.A. (ci-après, indistinctement, le « **Responsable du Traitement** » ou « **FSP** ») avec le code d'identification fiscale A-82798943 et l'adresse Camino de la Zarzuela, 1 - 28023, Madrid, en tant que société mère du groupe d'entreprises connu sous le nom d'Alsea Europe[6] , FSP étant responsable des chiffres du Responsable du Système d'Information Interne (ci-après, « **RSII** ») et du gestionnaire du canal d'information interne (ci-après, « **Gestionnaire du CII** ») d'Alsea Europe, organes internes d'Alsea Europe responsables du bon fonctionnement du système d'information interne (ci-après, « **SII** ») et de la gestion du canal d'information interne (ci-après, « **CII** »).

Les parties intéressées peuvent contacter le délégué à la protection des données d'Alsea Europe par courrier électronique à l'adresse dpd@alsea.net.

2. Finalités et légitimité du traitement

Les données à caractère personnel auxquelles on accède dans l'exercice des fonctions et des procédures régies par la présente Politique sont régies par les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommé « **RGPD** ») et les lois locales qui le transposent.

Dans les cas où vous choisissez de déposer une plainte de manière anonyme, FSP ne traitera aucune donnée personnelle à moins que vous ne choisissiez de la divulguer volontairement. Bien que le responsable du traitement s'efforce de garantir votre anonymat, veuillez noter que votre identité peut être déduite en fonction des spécificités de la plainte.

Si vous choisissez de divulguer votre identité, le PSF traitera vos données personnelles dans le but de traiter et de répondre aux plaintes reçues.

La base de légitimité de ce traitement dépend de la nature de la plainte déposée. En particulier, si les plaintes **(i)** se réfèrent à des activités ou à des omissions classées dans la loi national transposant la directive (UE) 2019/1937 ou qui peuvent être qualifiées d'infractions pénales ou d'infractions administratives graves ou très graves, le traitement sera fondé sur l'existence d'une obligation légale et sera donc soumis aux dispositions de l'article 6.1.c) du RGPD ; **(ii)**

[6] *Vous pouvez connaître les sociétés qui composent Alsea Europe en consultant la section 1 (Données d'identification) de l'avis juridique à l'adresse https://europe.alsea.net/legal.*

elles se réfèrent à des infractions autres que celles mentionnées ci-dessus, mais liées à des « actes ou comportements susceptibles de contrevenir à la réglementation générale ou sectorielle applicable » (par exemple, des infractions mineures), la base de légitimité du traitement sera l'intérêt public, tel qu'établi dans la loi relative à la protection des données personnelles, tombant ainsi dans le champ d'application de l'article 6.1.e) du RGDP ; et **(iii)** elles se réfèrent à des règlements internes qui n'impliquent pas d'infractions pénales ou administratives, la seule base de légitimation viable serait l'intérêt légitime, conformément à l'article 6.1.f) du RGDP. Dans de tels cas, vos données à caractère personnel seront traitées avec la plus grande confidentialité et toujours conformément au RGDP et à toute autre loi applicable en matière de protection des données.

En outre, le traitement des données à caractère personnel d'informations provenant de tiers serait justifié au titre de l'article 6, paragraphe 1, point f), du RGDP, c'est-à-dire l'intérêt légitime de la FSP à mener des enquêtes sur des activités contraires au droit national.

En outre, dans le cas de la réception de catégories particulières de données à caractère personnel de la part de plaignants ou de personnes concernées, la base légitime du traitement est l'article 6, paragraphe 1, point e), du RGDP (intérêt public) et l'exception à l'interdiction de traiter des catégories particulières de données à caractère personnel énoncée à l'article 9, paragraphe 2, point g), du RGDP (intérêt public essentiel).

3. Catégories de données à caractère personnel traitées et leur source d'origine

Le responsable du traitement peut traiter les données personnelles des informations suivants dans toutes les communications gérées par l'intermédiaire du CII :

- Les données d'identification, telles que le nom et le prénom, les coordonnées et les données relatives au statut de l'employé, telles que le poste ou le numéro d'employé, de la personne à signaler et de la personne qui fait le rapport.
- Relation avec Alsea Europe ou tout autre tiers concerné.
- Données relatives à la non-conformité signalée ou à la communication effectuée.
- Documentation pouvant fournir des preuves des faits rapportés.

Les données que le responsable du traitement peut traiter en raison de l'utilisation du CII proviennent des sources suivantes :

(i) Données fournies par les répondants via le CII.
(ii) Données générées à la suite du développement, du traitement et du maintien de la relation établie entre l'Informateur et le responsable du traitement des données.
(iii) Données personnelles (informations complémentaires) fournies par les sociétés du groupe Alsea Europe.
(iv) Données provenant de tiers ou de sources accessibles au public.

4. Communication de vos données personnelles

Vos données personnelles peuvent être divulguées à divers destinataires dans le but de prendre des mesures correctives au sein d'Alsea Europe ou pour le traitement des procédures disciplinaires ou pénales pertinentes.

À cet égard, le responsable du traitement peut les communiquer (i) aux forces et corps de sécurité de l'État, aux administrations publiques compétentes pour les actions signalées, aux tribunaux et autres organes juridictionnels, dans les cas prévus par la loi et aux fins qui y sont définies ; et (ii) aux sociétés du groupe Alsea Europe.

La base juridique de la communication de vos données aux entités indépendantes indiquées dans le paragraphe précédent dépendra de la nature de l'événement signalé. À cette fin, si la plainte concerne d'éventuelles violations de lois ou de règlements, la base juridique pour la communication de vos données à caractère personnel pourrait être le respect d'une obligation légale (article 6, paragraphe 1, point c), du RGPD) ou un intérêt public (article 6, paragraphe 1, point e), du RGPD). En revanche, si la plainte concerne le non-respect de règles internes qui n'impliquent pas d'infractions légales ou réglementaires, la base de légitime pourrait être un intérêt légitime (article 6, paragraphe 1, point f), du RGPD), à condition que cet intérêt ne l'emporte pas sur les droits et les intérêts des personnes concernées.

De même, d'autres prestataires de services peuvent avoir accès à vos données personnelles qui relèvent de la responsabilité de la FSP, en leur qualité de responsables du traitement des données (consultants et collaborateurs externes qui apportent leur soutien à la gestion ou, le cas échéant, à l'investigation des communications reçues par l'intermédiaire du CII et du prestataire de services qui permet la plateforme utilisée comme CII), avec lesquels FSP signera le contrat de traitement des données approprié (conformément à l'article 28 du RGPD).

Il n'y aura pas de transferts internationaux de vos données personnelles vers des pays tiers ou des organisations internationales.

5. Durée du traitement des données

Vos données seront conservées pendant la durée nécessaire à l'enquête sur les faits signalés, en tenant compte du fait que :

- Communication classée sans suite : si la communication ne respecte pas les exigences formelles, concerne un doute, une demande ou une plainte sans qu'il y ait infraction, est manifestement hors de propos ou ne présente aucun signe d'infraction, toutes les données seront supprimées du système.
- Communication admise pour enquête : vos données personnelles peuvent être conservées par le SII pendant la période minimale nécessaire pour évaluer le lancement d'une enquête sur la base des faits rapportés. Si les informations fournies, ou une partie d'entre elles, s'avèrent inexactes, elles devront être supprimées dès que cela se produira, sauf si l'inexactitude est susceptible de constituer une infraction pénale. Dans ce cas, les informations seront conservées aussi longtemps que nécessaire pendant toute la durée de la procédure judiciaire.
- En tout état de cause, si aucune mesure d'enquête n'a été prise dans les trois mois suivant la réception du rapport, celui-ci est supprimé, sauf si i) sa conservation a pour but de fournir des preuves d'irrégularités dans le fonctionnement du système de notification ; (ii) il est nécessaire de traiter les données à caractère personnel pendant une période plus longue afin de poursuivre l'enquête ou pour prouver le fonctionnement du SII ou parce qu'il est décidé d'engager une procédure disciplinaire et/ou judiciaire à l'encontre de la personne concernée, de la personne qui a fait la communication ou d'un tiers ; dans ce cas, les données peuvent être conservées pendant la durée requise par la législation applicable et ensuite, dûment bloquées, pendant les périodes de prescription des obligations légales applicables et de toute responsabilité découlant du traitement des données.

  Toutefois, lorsque des données à caractère personnel, y compris des catégories particulières de données, sont obtenues au cours de l'enquête et ne sont pas nécessaires aux fins de la connaissance et de l'investigation des faits, elles sont immédiatement supprimées du SII sans qu'aucun traitement ne soit effectué.

6. Droits

Les personnes concernées, dans les conditions établies par la réglementation applicable, ont le droit de demander l'accès à leurs données personnelles, leur rectification (si elles sont inexactes), leur suppression, la limitation du traitement ou l'opposition, de demander le droit à la portabilité des données (le cas échéant), ainsi que de ne pas faire l'objet de décisions fondées exclusivement sur le traitement automatisé de leurs données (le cas échéant) en envoyant une communication écrite au siège social de FSP en tant que société mère du groupe situé à Camino de la Zarzuela, 1 - 28023 Madrid, ou à l'adresse électronique du délégué à la protection des données d'Alsea Europe fournie à cet effet : dpd@alsea.net.

Ils ont également le droit de déposer une plainte auprès de l'autorité compétente en matière de protection des données dans chaque cas.

7. Mesures de sécurité

Dans le but de garantir la sécurité de vos données personnelles, le responsable du traitement s'engage à maintenir la sécurité et la confidentialité des données fournies et, en particulier, des données des utilisateurs qui effectuent une communication par l'intermédiaire du CII, en empêchant l'accès à ces données à ceux qui ont provoqué la communication en raison de l'infraction présumée au sein de l'organisation. À cette fin, le responsable du traitement a adopté les niveaux de sécurité légalement requis pour la protection des données personnelles et a utilisé les moyens techniques à sa disposition pour éviter la perte, l'utilisation abusive, l'altération, l'accès non autorisé et le vol de ces données, bien qu'il n'existe pas de sécurité absolue.

De même, le responsable du traitement vous informe que l'ensemble de notre personnel, quelle que soit la phase de traitement à laquelle il participe, s'engage à traiter vos données personnelles avec le plus grand soin et la plus grande confidentialité.

8. Mise à jour de la politique de confidentialité

Le responsable du traitement des données peut modifier sa politique de confidentialité conformément à la législation applicable à tout moment. C'est pourquoi il est conseillé de la lire chaque fois que vous accédez au site web ou que vous effectuez une procédure auprès de notre organisation.

ANNEXE II. Canaux d'information externes

1. En Espagne :

Sans préjudice de la nature préférentielle du CII d'Alsea Europe, les Informateurs, à condition que l'information ne puisse pas être traitée efficacement par Alsea Europe ou qu'elles comprennent qu'il existe un risque de représailles, peuvent signaler, y compris de manière anonyme, les violations visées au paragraphe 5.2 (i) de la politique par le biais du canal de signalement externe à :

a) L'Autorité Indépendante pour la Protection de l'Informateur (A.A.I.), lorsque l'infraction dénoncée affecte ou produit ses effets sur le territoire de plus d'une Communauté Autonome.

b) L'Autorité indépendante pour la protection de l'Informateur (A.A.I.) des Communautés autonomes, lorsque l'infraction signalée est limitée au territoire de la Communauté autonome correspondante.

En outre, ils peuvent signaler ces infractions aux autorités suivantes, entre autres :

a) Sur le travail et la santé et la sécurité des travailleurs :

(i) devant l'inspection du travail et de la sécurité sociale dans les matières relevant de sa compétence (travail, santé et sécurité au travail, sécurité sociale, emploi, etc.) À ces fins, les actions et omissions des responsables (personnes physiques ou morales et communautés de biens) sont considérées comme des infractions sociales et sont classées et sanctionnées dans les règlements d'ordre social.

(ii) Boîte aux lettres ITSS. Le ministère du travail et de l'économie sociale, par l'intermédiaire de l'agence nationale de l'inspection du travail et de la sécurité sociale, a mis à la disposition de tous les citoyens la « boîte aux lettres ITSS », où ils peuvent signaler (sans déposer de plainte formelle) certaines irrégularités en matière de travail dont ils ont connaissance. Dans ce cas, l'auteur du signalement ne doit pas fournir de données personnelles et la boîte aux lettres ne recueillera que des informations sur les irrégularités présumées dont il a connaissance.

b) Sur la protection des données :

(i) Par les différents canaux établis dans le siège électronique de l'AEPD : https://sedeagpd.gob.es/sede-electronica-web/

c) Sur la protection des consommateurs :

(i) Par l'intermédiaire de votre bureau municipal d'information des consommateurs ou de la direction générale de la consommation de votre communauté autonome https://www.consumo.gob.es/es/consumo/reclamaciones

d) En matière fiscale :

(i) Le canal des plaintes de l'Agence fiscale peut être utilisé pour signaler à l'Agence des faits ou des situations qui peuvent constituer des infractions fiscales ou de la contrebande, ou qui peuvent être importants pour l'application des taxes https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html.

2. En Belgique

La loi belge désigne l'Ombudsman fédéral (Médiateur fédéral) comme l'organe de coordination chargé de recevoir les communications et de les transmettre à l'organisme compétent dans le domaine ou le secteur concerné (comme l'Autorité des services et marchés financiers, la Banque nationale de Belgique et l'Autorité de protection des données).

3. En France

La loi française permet aux Informateurs de soumettre leur plainte externe à l'autorité compétente :

a) Les institutions compétentes de l'Etat désignées par le Conseil d'Etat.

b) Le « Défenseur des droits », qui à son tour transmettra le rapport à l'institution publique compétente.

c) L'autorité judiciaire.

d) Institutions, organes ou organisations de l'UE compétents pour recevoir des informations sur les infractions à la législation de l'UE.

4. Pays-Bas

Les autorités externes compétentes en vertu de la loi néerlandaise sont les suivantes :

a) L'Autorité des marchés et des consommateurs ;

b) L'autorité néerlandaise pour les marchés financiers ;

c) L'autorité néerlandaise de protection des données ;

d) De Nederlandsche Bank NV ;

e) L'inspection de la santé et de la jeunesse ;

f) La chambre des Informateurs ;

g) L'autorité sanitaire néerlandaise ;

h) Autorité de sûreté nucléaire et de radioprotection, et

i) Les organisations et les organismes administratifs, ou une partie d'entre eux, désignés par décret ou par règlement ministériel, qui ont des tâches ou des pouvoirs dans l'un des domaines visés à l'article 2, premier alinéa, de la directive.

5. Luxembourg

L'article 18 de la législation luxembourgeoise énumère les autorités compétentes auxquelles les Informateurs peuvent s'adresser. Ces autorités sont les suivantes

a) La Commission de surveillance du secteur financier.

b) Le Commissariat aux assurances.

c) L'Autorité de la concurrence.

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

e) L'inspection du travail et des mines.

f) La Commission nationale de protection des données.

g) Le Centre pour l'égalité de traitement.

h) Le Médiateur dans le cadre de sa mission de contrôle externe des lieux de privation de liberté.

i) Ombudsman fir Kanner a Jugendlecher.

j) L'Institut luxembourgeois de régulation.

k) L'Autorité luxembourgeoise indépendante de l'audiovisuel.

l) L'Ordre des avocats du Barreau de Luxembourg et l'Ordre des avocats du Barreau de Diekirch.

m) L'Ordre des notaires

n) L'Ordre des médecins.

o) Nature et gestion des forêts.

p) Administration de la gestion de l'eau.

q) L'administration de la navigation aérienne.

r) Le service national de médiation pour les consommateurs.

s) L'Ordre des architectes et des ingénieurs-conseils.

t) L'Ordre des experts-comptables.

u) L'Institut des réviseurs d'entreprises.

v) L'Administration des contributions directes.

6. Portugal

Les plaintes externes sont déposées auprès des autorités qui, en vertu de leurs pouvoirs et fonctions, devraient ou pourraient avoir connaissance de l'affaire faisant l'objet de la plainte, y compris :

a) Le ministère public.

b) Les forces de police criminelle.

c) La Banque du Portugal.

d) Autorités administratives indépendantes.

e) Instituts publics.

f) Les inspections générales et entités similaires et autres services centraux de l'administration directe de l'État dotés d'une autonomie administrative.

g) Autorités locales.

h) Partenariats publics.

7. Au niveau européen :

Les canaux externes auxquels les Informateurs peuvent s'adresser sont les suivants :

Sur la protection des données :

a) Via le portail du Comité européen de protection des données (CEPD), pour certaines questions https://edpb.europa.eu/about-edpb/more-about-edpb/contact-us_es

b) Sur le portail du Contrôleur européen de la protection des données (CEPD) https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en

Sur la protection des consommateurs :

a) Par le biais de la plateforme européenne http://ec.europa.eu/consumers/odr/.