Alsea

# Intern informatiesysteem (SII) Bedrijfsbeleid en bescherming Informanten

POL-CUMP-EUR-022

| Algemene beschrijving van het document | |
| --- | --- |
| **Titel van het document:** | Intern informatiesysteem (SII) Bedrijfsbeleid en bescherming Informanten |
| **Gebied:** | Compliance |
| **Macroproces:** | Regelgevend kader - Bedrijfsbeleid |
| **Proces:** | Compliance en risicobeheer |
| **Subproces:** | Naleving |
| **Toepassingsgebied:** | Europa |
| **Versie:** | 01 |
| **Datum laatste versie:** | 07/06/2024 |
| **Voorbereid door:** | *Compliance Officer* Alsea Europa |
| **Gerecenseerd door:** | Nalevingscommissie Alsea Europa |
| **Goedgekeurd door:** | Raad van bestuur van Alsea Europa |
| **Geverifieerd voor Interne Controle:** | Nalevingscommissie Alsea Europa |

| Versie register | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Versie** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Datum** | 07/06/2024 | | | | | | | |

# Inhoud

# 1. Doel

Zoals vastgelegd in de Ethische en Professionele Gedragscode van Alsea Europa[1] (hierna kortweg "***Alsea Europa***", de "***Onderneming***" of de "***Groep"***), moet elke werknemer[2] die bij Alsea Europa werkt en elke derde partij waarmee Alsea Europa een commerciële of professionele relatie heeft, zich integer gedragen en zijn of haar activiteiten uitvoeren in overeenstemming met de wet en de interne regels van Alsea Europa.

Evenzo is het de plicht van de voornoemde personen of entiteiten om bij het voorkomen en opsporen van onregelmatig of onwettig gedrag elke vermeende onregelmatigheid of handeling in strijd met de wet of interne regels waarvan zij kennis krijgen, te melden.

Met dit doel heeft Alsea Europa een intern meldingssysteem (hierna "**SII"**) opgezet in overeenstemming met de eisen die zijn vastgelegd in de wetten die van toepassing zijn op de ondernemingen waaruit Alsea Europa bestaat, waaronder Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 betreffende de bescherming van personen die schendingen van de wetten van de Unie melden (hierna "***Richtlijn 2019/1937***")[3] .

Dit Corporate SII en klokkenluidersbeschermingsbeleid (hierna, het "***Beleid***"), goedgekeurd door de Raad van Bestuur van FOOD SERVICE PROJECT, S.A. (hierna, "***FSP"***) getuigt enerzijds van het vaste voornemen van Alsea Europa om zich te houden aan goede bedrijfs-bestuurpraktijken en de ontwikkeling van een ethische en wettelijke nalevingscultuur, die bij haar belanghebbenden - zowel intern als extern - een geschikte informatie- en communicatiecultuur bevordert en versterkt als mechanisme dat ALSEA EUROPA helpt om onregelmatig gedrag te voorkomen en te identificeren en op deze manier hierop te kunnen reageren. Aan de andere kant stelt het de regels en algemene principes vast die het SII regelen, bestaande uit het geheel van menselijke, materiële en economische middelen gericht op het waarborgen van: (i) de bescherming van Informanten die overtredingen melden die vallen onder het toepassingsgebied van dit Beleid, (ii) evenals hun passende en effectieve behandeling.

# 2. Intern informatiesysteem (SII)

Alsea Europa's SII: (i) heeft een verantwoordelijke; (ii) integreert de verschillende interne informatiekanalen die binnen het bedrijf zijn opgezet; (iii) bevat een specifieke Procedure voor het Beheer van Ontvangen Informatie (hierna de "***Procedure***") die, om een interne informatiecultuur te bevorderen, de bescherming van de Informant garandeert en is goedgekeurd door de Raad van Bestuur van FSP; en (iv) is onafhankelijk van de interne informatiesystemen van andere entiteiten en organen.

---

*[1] In het kader van dit document wordt onder de bedrijvengroep "Alsea Europa" zowel FOOD SERVICE PROJECT, S.A. (FSP) verstaan als de bedrijven - nu of in de toekomst - waarvan FSP direct of indirect de meerderheid van de aandelen, aandelenbezit of stemrechten in handen heeft, of waarvan FSP een bestuurs- of leidinggevend orgaan heeft benoemd of de bevoegdheid heeft om een meerderheid van de leden te benoemen, zodanig dat FSP de feitelijke zeggenschap over het bedrijf heeft.*

*[2] In het kader van dit beleid worden werknemers gedefinieerd als alle werknemers die diensten verlenen aan de bedrijven die samen Alsea Europa vormen.*

*[3] In het kader van dit beleid is de wetgeving die van toepassing is op de ondernemingen waaruit Alsea Europa in deze kwestie bestaat: (i) België: De wet van 28 november 2022 betreffende de bescherming van klokkenluiders van inbreuken op de nationale wetgeving of de wetgeving van de Europese Unie gevestigd binnen een rechtspersoon uit de privésector, die in werking is getreden op 15 februari 2023; (ii) Frankrijk: Wet nr. 2022-401 van 21 maart 2022 ter verbetering van de bescherming van klokkenluiders; (iii) Nederland: Nederlandse wet tot gedeeltelijke omzetting van de richtlijn die op 18 februari 2023 in werking is getreden; iv) Luxemburg: wet van 16 mei 2023 tot omzetting van Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 betreffende de bescherming van personen die overtredingen van het recht van de Unie melden; v) Portugal: Wet nr. 93/2021 van 20 december 2021; en vi) Spanje: Wet nr. 2/2023 van 20 februari tot regeling van de bescherming van personen die overtredingen op de regelgeving en de bestrijding van corruptie melden.*

# 3. Gerelateerde documenten

| Code | Naam van het document |
| --- | --- |
| POL-CUMP-EUR-001 | Ethische code en Gedragscode |
| POL-CUMP-EUR-002 | Beleid ter bestrijding van corruptie |
| POL-CUMP-EUR-003 | Bedrijfsbeleid Belangenverstrengeling |
| POL-RH-EUR-001 | Beleid ter preventie van beroepsrisico's |
| POL-AJ-EUR-001 | Bedrijfsbeleid gegevensbescherming |
| POL-CUM-EUR-003 | Beleid inzake relatiegeschenken en uitnodigingen |
| POL-CUMP-EUR-005 | Beleid bedrijfsrisicobeheer |
| POL-CUMP-EUR-006 | Nalevingsbeleid |
| PRO-CUMP-EUR-009 | Procedure voor het beheer van ontvangen informatie |

# 4. Intern Informatie Systeem Manager (RSII) en Intern Informatie Kanaal Manager (CII)

De Raad van Bestuur van FSP heeft de Nalevingscommissie (hierna het "***RSII***") aangesteld als het orgaan dat verantwoordelijk is voor het toezicht op en het beheer van het SII, dat, als collegiaal orgaan, een manager van het Interne Meldkanaal zal benoemen van de leden van deze commissie (hierna de "***CII-Manager***" genoemd) .

Het begeleiden van, de supervisie over en de interpretatie van dit Beleid en de Procedure is, onverminderd de bevoegdheden die zijn voorbehouden aan de Raad van Bestuur van FSP, de verantwoordelijkheid van het RSII. Bovendien is het RSII verantwoordelijk voor het toezicht op de naleving ervan en, te zijner tijd, de interpretatie en het updaten ervan indien nodig of in het geval van organisatorische veranderingen, veranderingen van besturingsstructuur, van uitgevoerde activiteiten en/of wijzigingen in wetgeving of jurisprudentie.

Niettegenstaande het voorgaande mag de CII-Manager, in het kader van zijn functies en onverminderd de bevoegdheden van de RSII, uitvoeringsregels of handleidingen voor dit beleid en deze procedure opstellen die hij of zij nodig acht om de goede werking van het SII te waarborgen.

# 5. Openbaarmaking

## 5.1. Subjectief toepassingsgebied

Alsea Europa heeft haar SII opgezet als een openbaar communicatiekanaal dat beschikbaar is voor degenen:

(i) die werken of hebben gewerkt in de verschillende bedrijven die deel uitmaken van Alsea Europa (bijvoorbeeld: managers, werknemers, stagiairs, mensen in opleiding, etc.); of
(ii) die leden zijn of zijn geweest van het bestuur of de directie; of
(iii) die interactie hebben of hebben gehad, in het geheel of een deel van het commercieel proces, met of zonder betrokkenheid bij het bereiken van de doelstellingen en resultaten van Alsea Europa; of
(iv) externe partijen die een directe relatie en een legitiem en redelijk commercieel en/of professioneel belang hadden, hebben of kunnen hebben (aandeelhouder, klant, leverancier en hun werknemers, franchisenemers en hun werknemers, vrijwilligers, enz.)

Allen worden hierna gezamenlijk de "***Informanten***" genoemd.

## 5.2. Wat moet gerapporteerd worden via het interne informatiesysteem (SII)?

De SII is geen mailbox voor klachten- of ideeën, maar een systeem dat als doel heeft: (i) potentiële overtreders ontmoedigen; (ii) garanderen dat alle mogelijk onregelmatige handelingen kunnen worden gemeld en, indien nodig, naar behoren kunnen worden onderzocht; (iii) twijfels weg te nemen; en (iv) de nodige maatregelen te nemen om de bescherming te waarborgen van degenen die meewerken aan het melden en ophelderen van mogelijke overtredingen.

Met het oog op het voorgaande kunnen Informanten via het SII handelingen of nalatigheden melden die inbreuken of niet-nalevingen vormen in een arbeids- of beroepscontext en die betrekking hebben op elk van de bedrijven die deel uitmaken van de Groep op de volgende gebieden:

**(i)** **Overtredingen op EU- en lokale wetten die op Alsea** Europa **van toepassing zijn**:

a) Inbreuken op de wetgeving van de Europese Unie (EU), zolang als deze:

- invloed hebben op zaken als: overheidsopdrachten; financiële diensten, producten en markten, en het voorkomen van witwassen en terrorismefinanciering; productveiligheid; vervoersveiligheid; milieubescherming; consumentenbescherming; bescherming van de privacy en persoonsgegevens, en van netwerken en informatiesystemen;
- fraude of onwettige activiteiten vormen die de belangen van de Europese Unie schaden; of
- van invloed zijn op de interne markt[4], inclusief overtredingen op de mededingingsregels van de EU en de door lidstaten verleende steun, evenals overtredingen op de interne markt met betrekking tot handelingen die in strijd zijn met de regels inzake vennootschapsbelasting of praktijken die zijn gericht op het verkrijgen van een belastingvoordeel dat het doel of de strekking van de wetgeving inzake vennootschapsbelasting zou tenietdoen.

b) Strafbare feiten; en

c) Lichte, ernstige of zeer ernstige administratieve overtredingen.

Dit omvat in ieder geval alle overtredingen met betrekking tot intimidatie op het werk, seksuele intimidatie of intimidatie op grond van gender, en overtredingen met betrekking tot het werk en de gezondheid en veiligheid op het werk, evenals administratieve overtredingen die financieel verlies voor de staatskas en de sociale zekerheidsregelingen met zich meebrengen.

Bovenstaande strafrechtelijke en administratieve overtredingen vallen onder de bepalingen van de lokale wetgeving die van toepassing is op Alsea Europa.

**(ii)** **Andere nalevingsonregelmatigheden** die niet onder punt (i) vallen, in het bijzonder die in verband met het niet naleven van Alsea Europa's Ethische Code en Gedragscode of andere interne regels van Alsea Europa (bijv. beleid, protocollen, enz.).

**(iii)** **Adviezen over naleving van regelgeving**.

Alle mededelingen over overtredingen en vragen die via de SII worden ingediend, worden ontvangen door de CII-Manager. De CII-Manager is verantwoordelijk voor het beheer ervan, overeenkomstig met de Procedure voor het beheer van ontvangen informatie.

*[4] De interne markt omvat een ruimte zonder binnengrenzen waarin het vrije verkeer van goederen, personen, diensten en kapitaal is gewaarborgd volgens de bepalingen van de Verdragen.*

Met de implementatie van het interne informatiekanaal (hierna de "***CII***" genoemd) zijn de volgende kanalen geïntegreerd in de CII en dus niet langer van toepassing:

a) Het klokkenluider kanaal, en het e-mailadres canaletico@alsea.net worden gedeactiveerd.

b) Het Data Beschermingskanaal dpd@alsea.net voor overtredingen en schendingen van gegevensbescherming.

## 5.3. Welke communicatie is uitgesloten van het interne informatiesysteem (SII)?

Zoals hierboven vermeld, is het geen mailbox voor klachten of suggesties en moet het op een verantwoorde manier gebruikt worden, dusdanig zullen de volgende kwesties niet gecommuniceerd worden via dit kanaal:

a) Algemene informatie over Alsea Europa.
b) Klachten van commerciële aard of facturering.
c) Zaken waarvoor een specifiek kanaal bestaat (klantenservice, uitoefening van ARCO-POL-rechten, etc.).
d) Twijfels, vragen, claims en klachten van arbeids- of salarisaard.
e) Klachten over de faciliteiten of de staat van onderhoud.

Daartoe blijven de gewone kanalen beschikbaar voor mededelingen, verzoeken, vragen of opmerkingen met betrekking tot onder andere het volgende:

- Op de uitoefening van ARCO-POL-rechten[5] .
- Klantenservice.
- Externe communicatie.
- Verzoek om facturen.
- Talent en selectie.
- Werkgelegenheidskanalen.
- Kandidaten voor franchisenemers.

Informatie die via deze kanalen wordt gecommuniceerd, zal verder worden beheerd via de bestaande kanalen en middelen en in overeenstemming met hun specifieke procedures.

# 6. Soorten communicatie en communicatiemiddelen

## 6.1. Soorten communicatie

### 6.1.1.Raadplegingen

Het doel van de raadplegingen is om wijzigingen of verbeteringen voor te stellen of, indien van toepassing, vragen te stellen met betrekking tot Alsea Europa's Ethische Code en Gedragscode, andere interne regels van Alsea Europa of de toepasselijke wetgeving, of waarvan de toepassing twijfelachtig is, als het gaat om regels met betrekking tot naleving en/of misdaadpreventie.

Als u u zorgen maakt over een actie of gedrag dat van invloed kan zijn op de regels voor naleving en/of misdaadpreventie, moet dit ook als een vraag worden gemeld.

### 6.1.2.Klachten

Het doel van klokkenluiden is het melden van risico's of overtredingen van toepasselijke regels, zowel intern als wettelijk, in het bijzonder voor het melden van vermeende misdrijven, zoals aangegeven in punt 5.2 van dit beleid. Dit type communicatie kan worden gebruikt om misdrijven of overtredingen te melden die al zijn begaan of die te verwachten zijn op basis van

[5] *Het recht op toegang, rectificatie, annulering, verzet, overdraagbaarheid, afschaffing en beperking met betrekking tot gegevensbescherming*.

redelijke aanwijzingen, en zelfs het bestaan van onopgemerkte risico's die het begaan ervan zouden kunnen vergemakkelijken.

## 6.2. Communicatiemiddelen

Mededelingen kunnen gedaan worden via de volgende kanalen:

a) In eerste instantie, via de link die Alsea Europa beschikbaar maakt voor Informanten op de bedrijfswebsite.

b) Per gewone post naar Camino de la Zarzuela, 1, Madrid (28023) Spanje, ter attentie van de CII-Manager.

c) Persoonlijk, op verzoek van de Informant, hetzij door persoonlijke overhandiging van de schriftelijke klacht of mondeling, op het adres gelegen aan Camino de la Zarzuela, 1, Madrid (28023) Spanje, aan de CII-Manager, die verantwoordelijk zal zijn voor het bepalen van de voorwaarden waaronder de overhandiging zal plaatsvinden met oog op het behoud van de vertrouwelijkheid; en, in het geval van mondelinge communicatie, deze schriftelijk te verzamelen, voorzien van de handtekening van de Informant. Een online vergadering met de CII-Manager kan ook worden aangevraagd.

d) Uitsluitend van toepassing voor Spanje en voor gevallen van intimidatie op de werkplek, seksuele intimidatie of intimidatie op basis van gender, kan de klacht, naar keuze van de werknemer, worden ingediend bij de instanties die hiervoor zijn voorzien in de Procedure voor de preventie en behandeling van situaties van morele en seksuele intimidatie die van toepassing is op de Groep op lokaal niveau (louter als voorbeeld: de Instructiecommissie voor de behandeling van situaties van intimidatie, de arts die is toegewezen aan de preventiedienst, wettelijke vertegenwoordigers van de werknemers op de werkplek).

Alle mededelingen, ongeacht het kanaal waardoor ze worden gestuurd, moeten naar de CII-manager worden gestuurd, die verantwoordelijk zal zijn voor het invoeren ervan in de CII voor later beheer in overeenstemming met de bepalingen van dit beleid.

# 7. Inhoud van de communicatie

## 7.1. Raadplegingen

De raadpleging dient de specifieke aspecten van Alsea Europa's Ethische- en Gedragscode, eventuele andere interne regels of toepasselijke wetgeving te specificeren, mits er vragen zijn over de interpretatie en/of toepassing, wijzigingen of verbeteringen.

## 7.2. Klachten

Om de klacht ontvankelijk te maken, moeten de volgende punten, voor zover mogelijk, duidelijk worden aangegeven:

- Relatie van de Informant met Alsea Europa: Medewerker, Leverancier, Franchisenemer, Klant, enz.
- Een duidelijke en gedetailleerde beschrijving van de feiten of van het mogelijk onregelmatige gedrag, met bijzondere aandacht voor:
  - ✓ Datum of periode van de gebeurtenissen.
  - ✓ Middelen om het mogelijke/vermeende onwettige gedrag te plegen.
  - ✓ Als er andere personen zijn die meer informatie kunnen geven of hun getuigenis kunnen bevestigen.
  - ✓ Betrokken bedrijfssector of bedrijf.
- Indien mogelijk, identificatie van de personen die ervan worden verdacht verantwoordelijk te zijn voor de onregelmatigheid of, bij gebrek daaraan, vermelding van de gegevens aan de hand waarvan de identiteit van de van verantwoordelijkheid verdachte perso(o)n(en) kan worden vastgesteld.

- Verstrek, indien beschikbaar, van documenten of bewijsmateriaal met betrekking tot de ten laste gelegde feiten.
- Verklaring van de Informant dat hij/zij de mededeling over gegevensbescherming heeft gelezen en is geïnformeerd over de verwerking van zijn/haar persoonsgegevens in overeenstemming met de bepalingen van **bijlage I**.

Informanten worden gewaarschuwd dat ze moeten proberen informatie te verstrekken die nodig is om een bepaald feit te melden en dat ze moeten voorkomen dat ze overbodige of onnodige gegevens verstrekken (bijv. documenten die op onregelmatige wijze zijn verkregen of eigendom zijn van een derde partij, documenten die niet direct verband houden met de gemelde feiten, etc.). Als de melding niet de informatie bevat die nodig is om het onderzoek te starten, kan aanvullende informatie of documentatie worden gevraagd aan de Informant om te worden toegelaten voor verwerking.

Klachten met betrekking tot informatie die is uitgesloten van het toepassingsgebied van de SII, zijn niet ontvankelijk.

### 7.3. Verboden informatie

Alle communicatie die in strijd is met het rechtssysteem is uitgesloten van de SII, inclusief communicatie die van invloed is op gerubriceerde informatie en beroepsgeheimen, bijvoorbeeld die van de advocatuur en de vertrouwelijkheid van de veiligheidstroepen en -korpsen in het kader van hun acties.

## 8. Procedure voor het beheer van ontvangen informatie

Alle ontvangen vragen en klachten worden beheerd en verwerkt in overeenstemming met de toepasselijke regelgeving en in overeenstemming met de bepalingen van de Procedure.

Aangezien alle nalevingsovertredingen onder het SII vallen en derhalve in overeenstemming met de bepalingen van de Procedure zullen worden behandeld, zal de huidige versie van het Alsea Europa Klachten Kanaal Bedienings- en Beheerprotocol worden geannuleerd en vervangen door de huidige versie van het Alsea Europa Klachten Kanaal Bedienings- en Beheerprotocol.

Daarnaast omvat de bovengenoemde procedure de regels voor intimidatie op de werkplek, seksuele intimidatie of intimidatie op basis van gender die kunnen worden opgenomen in alle procedures voor de preventie en behandeling van situaties van morele en seksuele intimidatie die van toepassing kunnen zijn op de Groep op lokaal niveau.

### 8.1. Principes

De procedure die in dit beleid is ontwikkeld, is gebaseerd op de principes van vertrouwen, evenredigheid, onpartijdigheid, waarachtigheid en vertrouwelijkheid; op het recht op eer, het vermoeden van onschuld, het recht op verdediging, het recht om niet tegen zichzelf te getuigen en het recht op effectieve bescherming van de rechten van de Informant en de onderzochte persoon; en op de bescherming van de Informant tegen mogelijke represailles.

De procedure mag in geen geval in strijd zijn met de regels voor strafrechtelijke procedures, met inbegrip van onderzoeksprocedures.

### 8.2. Beheer van ontvangen informatie

Alle informatie die via de SII wordt gecommuniceerd, ongeacht het gebruikte kanaal of medium, wordt ontvangen door de CII-Manager.

De CII-Manager is verantwoordelijk voor het nemen van een besluit over: a) de toelating en verwerking of archivering van de ontvangen informatie; of b) de doorverwijzing naar de desbetreffende manager voor verwerking of archivering, in beide gevallen overeenkomstig de procedure.

Meldingen van intimidatie (op de werkplek of seksueel) moeten ontvangen worden door de CII-manager. In het geval van een strafrechtelijke overtreding wordt de melding behandeld door de CII-Manager en in het geval van een administratieve overtreding door een instantie die in dit verband kan worden ingesteld door de Procedure voor de preventie en behandeling van morele en seksuele intimidatiesituaties die van toepassing zijn op de Groep op lokaal niveau (bijv.: Commissie voor Onderzoek van Intimidatiesituaties (CITSA)). In elk geval is de Procedure van toepassing op deze informatie.

Binnen zeven (7) kalenderdagen na ontvangst van de informatie stuurt de CII-Manager de Informant een ontvangstbevestiging.

De CII-Manager beslist na de verzending van de ontvangstbevestiging over de toelating, de niet-ontvankelijkheid of de doorverwijzing van de informatie naar de bevoegde beheerder, afhankelijk van het onderwerp. In geval van toelating wordt de onderzochte partij(en) op de hoogte gebracht in overeenkomst met de bepalingen van de Procedure. In geen geval wordt de identiteit van de Informant meegedeeld aan de onderzochte(n), noch krijgen zij toegang tot de communicatie/klacht. In ieder geval zal de Informant op de hoogte worden gesteld van de toelating of afsluiting van de communicatie.

Het onderzoek valt onder de verantwoordelijkheid van de CII-manager die het, afhankelijk van het onderwerp van de mededeling, geheel of gedeeltelijk kan delegeren aan andere leden van de organisatie en/of aan externe adviseurs, zoals het geval kan zijn bij onderzoeken naar ernstige strafbare feiten, die kunnen worden uitbesteed aan gespecialiseerde externe adviseurs.

De afhandeling van het onderzoeksdossier mag niet langer duren dan drie (3) maanden vanaf de ontvangstbevestiging van de mededeling of, indien geen ontvangstbevestiging aan de Informant is gestuurd, drie (3) maanden vanaf het verstrijken van de periode van zeven (7) dagen na de mededeling, behalve in bijzonder gecompliceerde gevallen waarin het onderzoek met maximaal drie (3) extra maanden kan worden verlengd.

Deze tijdslimieten worden ingekort in geval van intimidatie op de werkplek, seksuele intimidatie of intimidatie op basis van gender, om te voldoen aan de tijdslimieten die in dit verband kunnen worden vastgelegd in procedures voor de preventie en behandeling van situaties van morele en seksuele intimidatie die van toepassing zijn op de Groep op lokaal niveau.

Zodra het onderzoek is afgerond, zal de instantie die het onderzoek heeft uitgevoerd een eindrapport met de conclusies van het onderzoek uitbrengen en, indien nodig, delen met de CII-Manager.

In gevallen van intimidatie op de werkplek, seksuele intimidatie of intimidatie op basis van gender, zal het bevoegde orgaan, zodra het onderzoek is afgerond en in overeenstemming met de Procedure, alle maatregelen nemen die passend zijn in overeenstemming met de Procedure voor de preventie en behandeling van situaties van morele en seksuele intimidatie die van toepassing is op de Groep op lokaal niveau.

Als uit de conclusies van het eindverslag van het onderzoek blijkt dat er sprake is van een vermoedelijke strafbare handeling waarvoor de Groep rechtstreeks strafrechtelijk aansprakelijk kan worden gesteld, wordt het eindverslag naar het RSII gestuurd, dat een besluit neemt over de te nemen disciplinaire en/of juridische maatregelen, evenals over de mogelijke mededeling aan de bevoegde gerechtelijke autoriteiten en/of het Openbaar Ministerie of het Europees Openbaar Ministerie, als de feiten de financiële belangen van de Europese Unie schaden.

De SII houdt een register bij van de ontvangen informatie en kent aan elk dossier een identificatiecode toe. Dit register is niet openbaar.

## 8.3. Rechten en garanties van Informanten

Informanten die overtredingen melden zoals beschreven in punt 5.2 van dit beleid, hebben recht op de volgende rechten en waarborgen:

a) Beslissen of de communicatie wel of niet anoniem gebeurt. In het geval dat de Informant kiest voor de niet-anonieme modaliteit, wordt de vertrouwelijkheid van zijn/haar identiteit gegarandeerd door zowel de RSII als door de CII-Manager en de personen die, indien van toepassing, tussenkomen bij de verwerking van de informatie.

b) De communicatie schriftelijk en/of mondeling formuleren. De geautoriseerde CII heeft een mechanisme dat identificatie door derden voorkomt.

c) Geïnformeerd te worden over de status van de verwerking en het resultaat van de communicatie. Daarom is het mogelijk om ervoor kiezen om meldingen of mededelingen te ontvangen met betrekking tot de toelating en verwerking van de informatie of uitdrukkelijk afstand doen van dit recht. In het geval dat de keuze gemaakt wordt om meldingen te ontvangen, kan de Informant ervoor kiezen om al dan niet een anoniem dialoog te onderhouden.

d) Verschijnen voor de Manager van de CII op eigen initiatief of op verzoek van de Manager, indien nodig bijgestaan door een advocaat.

e) De rechten van ARCO-POL uitoefenen met betrekking tot de bescherming van persoonsgegevens.

### 8.3.1. Recht op vertrouwelijkheid

De SII garandeert de vertrouwelijkheid van de identiteit van de Informant en van elke derde partij die in de communicatie wordt genoemd, evenals van de acties die worden uitgevoerd in het beheer en de verwerking ervan. Het garandeert ook de bescherming van gegevens en voorkomt toegang door onbevoegd personeel.

Ook wanneer een onder het SII vallende mededeling, of het nu een vraag of een klacht is, via een ander kanaal dan de CII wordt verzonden of wordt voorgelegd aan andere werknemers of vertegenwoordigers dan de RSII of de CII-Manager, zijn zij verplicht de vertrouwelijkheid ervan te waarborgen en deze onmiddellijk ter verwerking aan de CII-Manager te melden. Het niet nakomen van deze verplichting door de werknemer of vertegenwoordiger wordt beschouwd als een zeer ernstige inbreuk op dit beleid en dus als een inbreuk op hun arbeids- of contractuele verplichtingen.

De identiteit van de melder mag alleen in het kader van een strafrechtelijk, disciplinair of sanctieonderzoek aan de justitiële autoriteit, het Openbaar Ministerie of de bevoegde administratieve autoriteit worden meegedeeld. Voor openbaarmakingen op grond van dit kader gelden de waarborgen die zijn vastgelegd in de toepasselijke regelgeving. In het bijzonder wordt de Informant ingelicht voordat zijn of haar identiteit bekend gemaakt wordt, tenzij deze mededeling het onderzoek of de gerechtelijke procedure in gevaar zou kunnen brengen.

### 8.3.2. Recht op anonimiteit

De Informant kan beslissen of hij/zij de melding anoniem wil doen en daarom garandeert de SII anonieme toegang tot de CII zowel om de initiële klacht in te dienen als om met Alsea Europa te communiceren wanneer dit noodzakelijk is in het kader van het dossier dat geopend wordt naar aanleiding van de klacht.

### 8.3.3.Verbod op represailles

Het is ten strengste verboden om enige vorm van represailles, discriminatie en bestraffing toe te passen op grond van klachten die zijn ingediend tegen een Informant die te goeder trouw en op redelijke gronden de aandacht van Alsea Europa, via de SII, vraagt voor vermeend gedrag dat binnen het toepassingsgebied van de SII valt. Deze garantie strekt zich ook uit tot elke persoon die deelneemt aan het onderzoek (bv. getuigen, benadeelde partij, enz.), op voorwaarde dat hun tussenkomst te goeder trouw gebeurt.

Represailles worden geïnterpreteerd als elke handeling of nalatigheid die bij wet verboden is, of die, direct of indirect, leidt tot een ongunstige behandeling voor de persoon/personen die er het slachtoffer van is/zijn in de werk- of beroepscontext, uitsluitend vanwege zijn/haar status als Informant; op voorwaarde dat een dergelijke handeling of nalatigheid plaatsvindt

tijdens de onderzoeksfase of binnen twee (2) jaar na de voltooiing ervan. Een uitzondering wordt gemaakt in gevallen waarin een actie of nalatigheid objectief kan worden gerechtvaardigd in termen van een legitiem doel en waar de middelen die worden gebruikt om een dergelijk doel te bereiken noodzakelijk en passend zijn.

Als deze garantie wordt geschonden, moet dit worden gemeld voor onderzoek en als dit wordt bevestigd, kan de dader van de represailles worden onderworpen aan disciplinaire maatregelen.

Degenen die het volgende communiceren zijn uitdrukkelijk uitgesloten van de bescherming die in dit punt wordt geboden:

a) Informatie die eerder is gecommuniceerd via de CII en die is afgewezen.
b) Informatie die betrekking heeft op beweringen over interpersoonlijke conflicten of die alleen van invloed is op de Informant en de personen op wie de mededeling of bekendmaking betrekking heeft.
c) Informatie die al volledig beschikbaar is voor het publiek of die louter van horen zeggen is.
d) Informatie met betrekking tot handelingen of nalatigheden die niet vallen onder punt 5.2 van dit beleid.

Degenen die anoniem informatie hebben gemeld over overtredingen waarnaar wordt verwezen in punt 5.2 van dit beleid, maar vervolgens zijn geïdentificeerd en niet vallen onder de uitsluitingscriteria waarnaar hierboven wordt verwezen, hebben recht op bescherming tegen represailles.

### 8.3.4. Ter goede trouw handelen

Wanneer het onderzoek uitwijst dat de mededeling vals is en dat de Informant deze heeft gedaan met kennis van de onwaarheid ervan of met roekeloze veronachtzaming van de waarheid, kunnen strafrechtelijke, civielrechtelijke en/of disciplinaire maatregelen worden genomen, in overeenstemming met de voorwaarden van de huidige wetgeving en de disciplinaire regeling van Alsea Europa, en de vereisten van vertrouwelijkheid zullen ook worden opgeheven.

Het gebruik van de SII te kwader trouw is niet aanvaardbaar en misbruik van dit systeem zal betekenen dat gerechtelijke stappen genomen worden.

In deze zin wordt de Informant geacht te kwader trouw te handelen wanneer:

- De Informant bewust is van de onwaarheid van de feiten.
- De Informant handelt met flagrante minachting voor de waarheid.
- De Informant handelde met de wraakzuchtige intentie om de gerapporteerde persoon of het bedrijf schade te berokkenen.
- De Informant handelt met de intentie om de eer of de professionele, zakelijke of beroepsreputatie van een aan Alsea Europa verbonden persoon te ondermijnen.

## 8.4. Rechten van de onderzochte

De onderzochte persoon heeft het recht op het vermoeden van onschuld, het recht om zich te verdedigen, het recht op toegang tot het onderzoeksdossier en het recht op een doeltreffende bescherming van zijn of haar rechten. Te dien einde krijgt de onderzochte persoon een beknopte uiteenzetting van de feiten waarnaar een onderzoek is ingesteld, het recht om beschuldigingen te uiten en het bewijsmateriaal over te leggen dat hij of zij voor de verdediging nodig acht, en heeft hij/zij toegang tot het onderzoeksdossier, hoewel de identiteit van de Informant onder geen beding aan de onderzochte persoon mag worden medegedeeld, noch mag hen toegang worden verleend tot de klacht. Ook mag de onderzochte persoon zich laten bijstaan door een advocaat.

De onderzochte persoon heeft recht op dezelfde vertrouwelijkheid als voor Informanten, waarbij zijn of haar identiteit en de feiten en gegevens in het onderzoeksdossier worden beschermd.

### 8.5. Belangenverstrengeling

Indien de via de SII meegedeelde informatie gevolgen heeft voor de RSII of de CII-Manager en/of enige andere persoon die bij het beheer en de verwerking ervan betrokken zijn, wordt hun onthouding en absoluut verbod om deel te nemen in de verwerking (toelating, onderzoek en oplossing) van het onderzoek zoals ontwikkeld in de Procedure.

## 9. Externe kanalen

Het door Alsea Europa geïmplementeerde SII zal het kanaal bij uitstek zijn voor het melden van de in punt 5.2 (i) van dit beleid vermelde handelingen of nalatigheden, op voorwaarde dat de persoon die de melding maakt van mening is dat de overtreding doeltreffend kan worden aangepakt en dat er geen risico op represaille bestaat. **Bijlage II** van dit beleid bevat, bij wijze van voorbeeld maar niet beperkt tot, bepaalde externe kanalen in de landen waarin Alsea Europa actief is. Niettegenstaande het voorgaande zijn de werknemers van Alsea Europa verplicht om via het SII elke overtreding op de in punt 5.2(ii) vermelde interne regels te melden wanneer deze geen overtreding vormt op de in punt 5.2(i) vermelde regels.

### 9.1. Samenwerking met de autoriteiten

Alsea Europa zal, op voorwaarde dat haar recht op verdediging en het recht om niet tegen zichzelf te getuigen niet in het gedrang komen, met de grootst mogelijke zorgvuldigheid samen te werken met en/of reageren op verzoeken van de administratieve en gerechtelijke autoriteiten, het Openbaar Ministerie of het Europees Openbaar Ministerie met betrekking tot handelingen die verband houden met Alsea Europa of om enige andere reden. De aandacht voor deze eisen zal worden beheerd door het nalevingscomité, dat onmiddellijk de raad van bestuur van FSP op de hoogte moet stellen, op voorwaarde dat de feiten die aanleiding gaven tot het communiceren van de melding, kunnen leiden tot directe strafrechtelijke aansprakelijkheid voor de Groep.

## 10. Bescherming van persoonlijke gegevens

Bij het beheer van de SII worden de toepasselijke wettelijke voorschriften inzake de bescherming van persoonsgegevens nageleefd, waarvoor de "Informatie over de verwerking van persoonsgegevens" in ***bijlage I is opgenomen***.

## 11. Niet-naleving

Elke overtreding van dit beleid door werknemers van Alsea Europa zal worden geanalyseerd in overeenstemming met interne procedures, wettelijke voorschriften en geldende wederzijdse overeenkomsten en, indien van toepassing, zullen de bijbehorende disciplinaire maatregelen worden toegepast op de overtreder, onverminderd eventuele andere aansprakelijkheden (strafrechtelijk of anderszins) die de overtreder heeft opgelopen.

## 12. Distributie en accordatie

Dit beleid is beschikbaar voor alle werknemers die deel uitmaken van Alsea Europa, evenals voor derden, door publicatie op de bedrijfswebsite.

Alsea Europa zal de nodige maatregelen nemen om al haar werknemers bekend te maken met , op te leiden en te informeren over de SII, haar principes, garanties en verplichtingen, evenals haar doel.

Dit beleid is goedgekeurd door de Raad van Bestuur van FSP op 11 van Juni van 2024, met ingang van die datum.

# BIJLAGE I. Informatie over de verwerking van persoonsgegevens

**BASISGEGEVENSBESCHERMING (EERSTE LAAG)**

**Verantwoordelijke voor de verwerking**: FOOD SERVICE PROJECT, S.A.

**Doel**: Het beheren van de informatie die via de CII wordt verwerkt.

**Rechten**: Indien nodig kunt U uw recht op toegang, rectificatie, verwijdering, oppositie, portabiliteit, begrenzing, evenals het recht om niet te worden onderworpen aan geautomatiseerde individuele besluiten, uitoefenen door te schrijven naar dpd@alsea.net of naar het postadres Camino de la Zarzuela, 1. Madrid (Spanje). U kunt ook een klacht indienen bij de bevoegde toezichthoudende autoriteit voor gegevensbescherming.

**Aanvullende informatie**: U kunt aanvullende en gedetailleerde informatie raadplegen door te klikken op het "Privacybeleid" dat voor deze specifieke behandeling is opgesteld.

**PRIVACYBELEID EN AANVULLENDE INFORMATIE OVER GEGEVENSBESCHERMING (TWEEDE NIVEAU)**

**1. Gegevensbeheerder en contactgegevens van de functionaris voor gegevensbescherming**

In overeenstemming met de regelgeving met betrekking tot de bescherming van persoonsgegevens wordt FOOD SERVICE PROJECT, S.A. (hierna, zonder onderscheid, de "**Verwerkingsverantwoordelijke**" of "**FSP**") beschouwd als de verantwoordelijke voor de verwerking van de gegevens, met belastingnummer A-82798943 en adres Camino de la Zarzuela, 1 - 28023, Madrid, als moedermaatschappij van de groep bedrijven bekend als Alsea Europa[6] , waarbij FSP verantwoordelijk is voor de functies van de Manager van het Interne Informatie Systeem (hierna, **"RSII**") en die van de Manager van het Interne Informatiekanaal (hierna "**CII-Manager**") van Alsea Europa, interne instanties van Alsea Europa die verantwoordelijk zijn voor de correcte werking van het Interne Informatiesysteem (hierna "**SII**") en het beheer van het Interne Informatiekanaal (hierna **"CII**").

Geïnteresseerde partijen kunnen per e-mail contact opnemen met de functionaris voor gegevensbescherming van Alsea Europa via dpd@alsea.net.

**2. Doeleinden en rechtmatigheid van de verwerking**

Persoonsgegevens waartoe toegang wordt verkregen bij de uitvoering van de functies en procedures die in dit Beleid worden geregeld, zijn onderworpen aan de voorschriften van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna "**AVG**") en de lokale wetten die van toepassing zijn.

In gevallen waarin u ervoor kiest om een klacht anoniem in te dienen, zal FSP geen persoonlijke gegevens verwerken, tenzij u ervoor kiest om deze vrijwillig vrij te geven. Hoewel de verantwoordelijke van de verwerking ernaar streeft om uw anonimiteit te waarborgen, dient u er rekening mee te houden dat uw identiteit kan worden afgeleid op basis van de specifieke kenmerken van de klacht.

Als u ervoor kiest om uw identiteit bekend te maken, zal FSP uw persoonlijke gegevens verwerken met als doel het behandelen van en reageren op ontvangen klachten.

De legitimiteit van deze verwerking is afhankelijk van de aard van de ingediende klacht. Specifiek, als de klachten **(i) betrekking** hebben op activiteiten of nalatigheden die worden geclassificeerd in de nationale wetgeving tot omzetting van Richtlijn (EU) 2019/1937 of die kunnen worden geclassificeerd als strafbare feiten of ernstige of zeer ernstige administratieve

*[6] U kunt meer te weten komen over de bedrijven die deel uitmaken van Alsea Europa door deel 1 (Identificatiegegevens) van de Wettelijke Bekendmaking op https://europe.alsea.net/legal te raadplegen.*

misdrijven, zal de verwerking gebaseerd zijn op het bestaan van een wettelijke verplichting, en zal daarom onderworpen zijn aan de bepalingen van artikel 6.1. van de AVG; **(ii) betrekking** hebben op andere strafbare feiten dan de bovengenoemde, maar gerelateerd zijn aan "handelingen of gedrag dat in strijd kan zijn met de toepasselijke algemene of sectorale regelgeving" (bijv. minder ernstige strafbare feiten), de basis voor de legitimiteit van de gegevensverwerking komt voort uit het algemeen belang, zoals vastgesteld in de wetgeving gegevensbescherming, en valt dus onder het toepassingsgebied van artikel 6.1.e) van de AVG; en **(iii) verwijzen** naar interne regelgeving die geen betrekking heeft op strafrechtelijke of administratieve overtredingen, in dit geval zou de rechtmatigheid van de behandeling gebaseerd zijn op het algemeen belang, in overeenstemming met artikel 6.1.f) van de AVG. In dergelijke gevallen worden uw persoonlijke gegevens met de grootst mogelijke vertrouwelijkheid en altijd in overeenstemming met de AVG en andere toepasselijke wetgeving inzake gegevensbescherming behandeld.

Daarnaast zou de verwerking van persoonsgegevens van informatie van derden gerechtvaardigd zijn op grond van artikel 6, lid 1, punt f), van de AVG, wat neerkomt op een gerechtvaardigd belang van FSP bij het uitvoeren van onderzoeken naar activiteiten die in strijd zijn met de nationale wetgeving.

In het geval van de ontvangst van bijzondere categorieën persoonsgegevens van klagers of betrokkenen, is de legitieme grondslag voor de verwerking artikel 6, lid 1, punt e) van de AVG (algemeen belang), en de uitzondering op het verbod op de verwerking van bijzondere categorieën persoonsgegevens van artikel 9, lid 2, punt g) van de AVG (essentieel algemeen belang).

## 3. Categorieën van verwerkte persoonsgegevens en hun bron van herkomst

De verantwoordelijke van de verwerking mag persoonsgegevens van de volgende soorten informatie verwerken in alle communicatie die via de CII wordt beheerd:

- Identificerende gegevens, zoals naam en achternaam, contactgegevens en gegevens met betrekking tot de status van de werknemer, zoals functie of werknemersnummer, van zowel de persoon die gerapporteerd moet worden als de persoon die rapporteert.
- Relatie met Alsea Europa of andere betrokken derde partij.
- Gegevens met betrekking tot de gerapporteerde niet-naleving of de gedane mededeling.
- Documentatie die bewijs kan leveren voor de feiten die worden gerapporteerd.

De gegevens die de verantwoordelijke kan verwerken als gevolg van het gebruik van de CII zijn afkomstig van de volgende bronnen:

(i) Gegevens verstrekt door respondenten via de CII.
(ii) Gegevens die worden gegenereerd als gevolg van de ontwikkeling, de verwerking en het onderhoud van de relatie tussen de Informant en de verantwoordelijke voor de verwerking.
(iii) Persoonlijke gegevens (aanvullende informatie) verstrekt door bedrijven van de Alsea Europa groep.
(iv) Gegevens van derden of openbaar beschikbare bronnen.

## 4. Communicatie van uw persoonlijke gegevens

Uw persoonlijke gegevens kunnen aan verschillende ontvangers worden doorgegeven voor het nemen van corrigerende maatregelen binnen Alsea Europa of voor de afhandeling van de betreffende disciplinaire of strafrechtelijke procedures.

In dit verband kan de verantwoordelijke van de verwerking ze mededelen (i) aan de staatsveiligheid- en Opsporingsdiensten , overheidsdiensten met rechtsbevoegdheid over de gemelde zaken, gerechtshoven en andere bevoegde instanties, in de gevallen waarin de wet voorziet en voor de daarin omschreven doeleinden ; en (ii) aan de bedrijven van de Alsea Europa groep.

De rechtsgrondslag voor de communicatie van uw gegevens aan de onafhankelijke entiteiten die in de vorige paragraaf genoemd werden, is afhankelijk van de aard van de gemelde gebeurtenis. Als de klacht betrekking heeft op mogelijke overtredingen van wet- of regelgeving, kan de rechtsgrondslag voor de communicatie van uw persoonsgegevens het voldoen van een wettelijke verplichting zijn (artikel 6, lid 1, punt c) van de AVG) of een algemeen belang zijn (artikel 6, lid 1, punt e) van de AVG). Aan de andere kant, als de klacht betrekking heeft op het niet naleven van interne regels die geen wettelijke of reglementaire overtreding inhouden, zou de basis voor legitimatie een gerechtvaardigd eigenbelang kunnen zijn (Artikel 6, lid 1, punt f van de AVG), op voorwaarde dat dergelijke belangen niet zwaarder wegen dan de rechten en belangen van de betrokkenen.

Evenzo kunnen andere dienstverleners toegang hebben tot uw persoonsgegevens die onder de verantwoordelijkheid van FSP vallen, in hun hoedanigheid van gegevensverwerkers (adviseurs en externe medewerkers die ondersteuning bieden bij het beheer of, indien van toepassing, het onderzoek van de communicatie die wordt ontvangen via de CII en de dienstverlener van het platform die het mogelijk maakt dat deze gebruikt wordt als CII), met wie FSP het toepasselijke gegevensverwerkingscontract zal ondertekenen (in overeenstemming met artikel 28 van de AVG).

Er vindt geen internationale overdracht van uw persoonlijke gegevens naar derde landen of internationale organisaties plaats.

## 5. Duur van de gegevensverwerking

Uw gegevens worden bewaard gedurende de tijd die nodig is voor het onderzoek naar de gemelde feiten, rekening houdend met het feit dat:

- Mededeling zonder actie: als de mededeling niet voldoet aan de formele eisen, twijfel betreft, een vraag of klacht betreft zonder dat er sprake is van een overtreding, duidelijk irrelevant is of geen aanwijzingen bevat dat er sprake is van een overtreding, worden alle gegevens uit het systeem verwijderd.
- Mededeling toegelaten voor onderzoek: uw persoonsgegevens kunnen door de SII bewaard worden gedurende de minimumperiode die nodig is om te beoordelen of een onderzoek wordt ingesteld op basis van de gemelde feiten. Als de verstrekte informatie, of een deel daarvan, onjuist blijkt te zijn, moet deze onmiddellijk worden verwijderd zodra dit duidelijk wordt, tenzij de onjuistheid een strafbaar feit zou kunnen vormen. In dat geval wordt de informatie zo lang bewaard als nodig is tijdens de relevante gerechtelijke procedure.
- Als er binnen drie maanden na ontvangst van de melding geen onderzoeksmaatregel is genomen, wordt de melding in elk geval verwijderd, tenzij i) het doel van het bewaren ervan is om bewijs te leveren van onregelmatigheden in de werking van het meldsysteem; (ii) het noodzakelijk is de persoonsgegevens gedurende een langere periode te verwerken om het onderzoek voort te zetten of om het functioneren van het SII aan te tonen of omdat wordt besloten een disciplinaire en/of gerechtelijke procedure in te leiden tegen de betrokken persoon, de persoon die de melding heeft gemaakt of een derde; in dat geval mogen de gegevens worden bewaard gedurende de periode die is voorgeschreven door de toepasselijke wetgeving en daarna, naar behoren afgeschermd, gedurende de verjaringstermijnen van de toepasselijke wettelijke verplichtingen en van eventuele aansprakelijkheden die voortvloeien uit de verwerking van de gegevens.

  Wanneer echter in de loop van het onderzoek persoonsgegevens, met inbegrip van bijzondere categorieën gegevens, worden verkregen die niet noodzakelijk zijn voor de kennis en het onderzoek van de feiten, worden zij onmiddellijk uit de SII verwijderd zonder dat enige verwerking plaatsvindt.

## 6. Rechten

Betrokkenen hebben, onder de voorwaarden die zijn vastgelegd in de toepasselijke regelgeving, het recht om toegang te vragen tot hun persoonlijke gegevens, de rectificatie ervan (indien onjuist), de verwijdering ervan, beperking van de verwerking of oppositie, het recht op gegevensoverdraagbaarheid (indien van toepassing), alsook om niet onderworpen te

worden aan besluiten die uitsluitend gebaseerd zijn op de geautomatiseerde verwerking van hun gegevens (indien van toepassing) door een schriftelijke mededeling te sturen naar de maatschappelijke zetel van FSP als moedermaatschappij van de groep gevestigd te Camino de la Zarzuela, 1 - 28023 Madrid, of naar het e-mailadres van de Gegevensbescherming Beheerder van Alsea Europa dat voor dit doel is verstrekt: dpd@alsea.net.

Betrokkenen hebben ook het recht om in elk geval een klacht in te dienen bij de bevoegde gegevensbeschermingsautoriteit.

## 7. Veiligheidsmaatregelen

Teneinde de veiligheid van uw persoonsgegevens te waarborgen, verbindt de verantwoordelijke voor de verwerking zich ertoe de veiligheid en vertrouwelijkheid van de verstrekte gegevens te handhaven en in het bijzonder van de gegevens van gebruikers die via de CII een mededeling maken, waarbij wordt voorkomen dat degenen die de mededeling hebben gemaakt, toegang tot deze gegevens krijgen vanwege de vermeende overtreding binnen de organisatie. Daartoe heeft de verantwoordelijke voor de verwerking de wettelijk vereiste beveiligingsniveaus voor de bescherming van persoonsgegevens ingevoerd en de technische middelen gebruikt die tot zijn of haar beschikking staan om verlies, misbruik, wijziging, ongeoorloofde toegang en diefstal van deze gegevens te voorkomen, hoewel absolute veiligheid niet bestaat.

Evenzo informeert de verantwoordelijke voor de verwerking u dat al onze medewerkers, ongeacht de fase van de verwerking waarbij zij betrokken zijn, verplicht zijn om uw persoonsgegevens met de grootst mogelijke zorgvuldigheid en vertrouwelijkheid te behandelen.

## 8. Update privacybeleid

De verantwoordelijke voor de verwerking kan het Privacybeleid op elk moment wijzigen in overeenstemming met de geldende wetgeving. Daarom is het raadzaam om het te lezen telkens wanneer u de website bezoekt of een procedure met onze organisatie uitvoert.

# BIJLAGE II. Externe informatiekanalen

**1. In Spanje:**

Zonder afbreuk te doen aan het voorkeurskarakter van de CII van Alsea Europa, mogen Informanten, op voorwaarde dat de informatie niet doeltreffend kan worden behandeld door Alsea Europa of zij begrijpen dat er een risico bestaat op represailles, mogen Informanten, ook anoniem, de in punt 5.2 (i) van het Beleid gereguleerde schendingen via het Externe Meldingskanaal melden aan:

a) De Onafhankelijke Instantie voor de Bescherming van de Informant (A.A.I.), wanneer de gemelde overtreding invloed of gevolgen heeft binnen het territoriale bereik van meer dan één Autonome Regio.

b) De Onafhankelijke Instantie voor de Bescherming van de Informant (A.A.I.) van de Autonome Regio's, wanneer de gemelde overtreding beperkt is tot het territoriale bereik van de betreffende Autonome Regio.

Daarnaast kunnen ze deze overtredingen melden bij onder andere de volgende instanties:

a) Over arbeid en gezondheid en veiligheid van werknemers:

(i) Voor de arbeids- en sociale zekerheidsinspectie in zaken die onder haar bevoegdheid vallen (arbeid, gezondheid en veiligheid op het werk, sociale zekerheid, werkgelegenheid, enz.). Voor deze doeleinden worden de handelingen en nalatigheden van de verantwoordelijke partijen (natuurlijke of rechtspersonen en gemeenschappelijke eigendommen) beschouwd als sociale overtredingen en worden ze geclassificeerd en gesanctioneerd in de sociale regelgeving.

(ii) ITSS Mailbox. Het ministerie van Arbeid en Sociale Economie heeft via het Staatsagentschap van de Arbeids- en Sociale Zekerheidsinspectie aan alle burgers de "ITSS-mailbox" ter beschikking gesteld, waar ze bepaalde onregelmatigheden, op het gebied van arbeid, waarvan ze op de hoogte zijn kunnen melden (geen formele klachten). In dit geval hoeft de melder geen persoonlijke gegevens te verstrekken en zal de mailbox alleen informatie verzamelen over de vermeende onregelmatigheden waarvan hij/zij op de hoogte is.

b) Over gegevensbescherming:

(i) Via de verschillende kanalen van het elektronische hoofdkantoor van het AEPD: https://sedeagpd.gob.es/sede-electronica-web/

c) Over consumentenbescherming:

(i) Via het plaatselijke gemeentelijke bureau voor consumentenvoorlichting of het directoraat-generaal Consumentenzaken van uw autonome regio https://www.consumo.gob.es/es/consumo/reclamaciones

d) Op belastinggebied:

(i) Het klachtenkanaal van de belastingdienst kan worden gebruikt om feiten of situaties aan de dienst te melden die mogelijk een fiscale overtreding of smokkel vormen, of die van belang kunnen zijn voor de toepassing van belastingen https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html.

**2. In België**

De Belgische wet wijst de Federale Ombudsman (Federale Bemiddelaar) aan als coördinerend orgaan dat verantwoordelijk is voor het ontvangen van meldingen en het doorsturen ervan naar de specifieke instantie of de verantwoordelijke sectorinstantie (zoals de Autoriteit voor Financiële Diensten en Markten, de Nationale Bank van België en de Gegevensbeschermingsautoriteit).

### 3. In Frankrijk

Volgens de Franse wet kunnen Informanten hun externe klacht indienen bij:

a) De bevoegde staatsinstellingen aangewezen door de toekomstige Raad van State.

b) Decreten van de Raad van State.

c) De Franse instelling genaamd de "Verdediger van de Rechten", die op zijn beurt het rapport zal doorsturen naar de bevoegde staatsinstelling.

d) De gerechtelijke autoriteit.

e) EU-instellingen, -organen of -organisaties die bevoegd zijn om informatie te ontvangen over overtredingen op de wetgeving van de EU.

f) Federale bemiddelaars.

### 4. Nederland

De bevoegde externe autoriteiten in overeenstemming met de Nederlandse wet zijn:

a) De Autoriteit Consument en Markt;

b) De Autoriteit Financiële Markten;

c) Het College Bescherming Persoonsgegevens;

d) De Nederlandsche Bank NV;

e) De Inspectie Gezondheidszorg en Jeugd;

f) Het Huis voor Klokkenluiders;

g) De Nederlandse Zorgautoriteit;

h) De Autoriteit voor nucleaire veiligheid en stralingsbescherming, en

i) De bij algemene maatregel van bestuur of ministeriële regeling aangewezen organisaties en bestuursorganen, of onderdelen daarvan, die taken of bevoegdheden hebben op een van de in artikel 2, eerste punt, van de Richtlijn

### 5. Luxemburg

Artikel 18 van de Luxemburgse wetgeving somt de bevoegde autoriteiten op tot wie informanten zich kunnen wenden. Dit zijn:

a) De Commissie van toezicht op de financiële sector.

b) Het Commissariat aux assurances.

c) De mededingingsautoriteit.

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

e) De Arbeids- en Mijneninspectie.

f) De nationale commissie voor gegevensbescherming.

g) Het Centrum voor Gelijke Behandeling.

h) De Ombudsman in het kader van de opdracht tot externe controle op gevallen van vrijheidsberoving.

i) Ombudsman fir Kanner aan Jugendlecher.

j) Het Institut luxembourgeois de régulation.

k) De Autorité luxembourgeoise indépendante de l'audiovisuel.

l) De Ordre des avocats du Barreau de Luxembourg en l'Ordre des avocats du Barreau de Diekirch.

m) De orde der Notarissen en De orde der Artsen

n) Natuur en bosbeheer.

o) Administratie waterbeheer.

p) De Luchtvaartnavigatiedienst.

q) De Nationale Ombudsman voor Consumenten.

r) De Ordre des architectes et des ingénieurs-conseils.

s) De Ordre des experts-comptables.

t) Het Institut des réviseurs d'entreprises.

u) De Administration des contributions directes.

**6. Portugal**

Externe klachten moeten ingediend worden bij de autoriteiten die op basis van hun bevoegdheden en taken op de hoogte moeten of kunnen zijn van de zaak waarover een klacht is ingediend, waaronder:

a) Het Openbaar Ministerie.

b) Politiediensten.

c) De Bank van Portugal.

d) Onafhankelijke administratieve autoriteiten.

e) Openbare instellingen.

f) De Algemene Inspectie van diensten en soortgelijke entiteiten en andere centrale diensten van de directe overheidsadministratie met bestuurlijke autonomie.

g) Lokale autoriteiten.

h) Publieke partnerschappen.

**7. Op Europees niveau:**

De externe kanalen waartoe Informanten zich kunnen wenden zijn onder andere:

Over gegevensbescherming:

a) Via het portaal van het Europees Comité voor gegevensbescherming (EDPB), voor bepaalde kwesties https://edpb.europa.eu/about-edpb/more-about-edpb/contact-us_es

b) Via het portaal van de Europese Toezichthouder voor gegevensbescherming (EDPS) https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en

Over consumentenbescherming:

a) Via het Europese platform http://ec.europa.eu/consumers/odr/.