



## Politique Lanceur d’Alerte

### Contenu

Objectif de cette politique .....	2	Sécurité .....	8
Champ d'application .....	2	Protection contre les représailles.....	9
Utilisation volontaire du dispositif d’Alerte Interne .....	3	Protection des données personnelles .....	9
Ce qui peut être signalé .....	3	Signalements externes.....	10
Comment signaler .....	4	Modification de la présente politique .....	10
Signalement anonyme .....	5	Questions concernant cette politique.....	10
Traitement des signalements .....	5	A. Annexes par pays .....	11
Confidentialité .....	7	FRANCE .....	11
		B. Déclaration de confidentialité .....	13



## Objectif de cette politique

---

Euroports s'engage à maintenir un niveau élevé d'intégrité, de transparence et de comportement éthique. Le respect et l'intégrité sont des valeurs fondamentales de notre organisation.

Il est dans l'intérêt d'Euroports et de son personnel de s'attaquer correctement et rapidement aux comportements répréhensibles. Cela nous permet de prévenir des dommages plus importants, d'éviter d'entacher notre réputation et de demander des comptes aux responsables.

Cette politique offre des canaux de communication confidentiels pour signaler des préoccupations concernant des comportements illégaux ou contraires à l'éthique au sein de notre organisation, sans crainte de représailles.

Ces voies de signalement s'ajoutent à la possibilité de discuter de manière informelle avec votre supérieur hiérarchique, les RH, le service juridique, le service QHSE ou d'autres collègues concernés ou, pour les personnes ne faisant pas partie du personnel, avec votre personne de contact au sein d'Euroports.



Il est important que toute faute (éventuelle) soit signalée, afin qu'Euroports puisse s'attaquer au problème.

Se taire en cas de mauvaise conduite peut aggraver la situation. Signaler les problèmes contribue à une culture d'entreprise responsable et positive.

Pour les entités de l'UE, cette politique constitue également une mise en œuvre de la directive 2019/1937 de l'UE "relative à la protection des personnes qui signalent des violations du droit de l'Union" et de la législation nationale de mise en œuvre correspondante, dans les limites de leur champ d'application.



## Champ d'application

---

Cette politique est applicable à toutes les entités du groupe Euroports.

Il s'applique à **toutes les personnes qui entrent en contact avec Euroports dans un contexte professionnel**, c'est-à-dire

- toutes les personnes travaillant pour les entités d'Euroports, y compris ses employés, consultants, consultants de projet, travailleurs temporaires ou intérimaires, stagiaires et cadres (ci-après dénommés conjointement "**membres du personnel**") ; et

- toutes les **autres** personnes ayant une relation professionnelle actuelle, passée ou future avec Euroports, y compris les anciens membres du personnel, les candidats à l'emploi, les actionnaires, les membres du conseil d'administration, le personnel des fournisseurs, le personnel des clients, les dockers (s'ils ne sont pas employés par Euroports), etc ;

(désignés conjointement dans la présente politique par "vous" ou "le Lanceur d'Alerte").



## Utilisation volontaire du dispositif d'Alerte Interne

---

Nous vous encourageons à vous exprimer et à discuter de toute préoccupation concernant un comportement potentiellement illégal ou contraire à l'éthique.

L'utilisation de la procédure de signalement décrite dans la présente politique est toutefois totalement volontaire.

Au lieu d'utiliser le dispositif d'Alerte Interne, vous êtes libre de faire part de vos préoccupations à :

- votre superviseur/responsable ;
- le service des ressources humaines, le service juridique ou le service QHSE ;
- un autre collègue compétent ; ou
- votre personne de contact chez Euroports.



## Ce qui peut être signalé

---



Notre dispositif d'Alerte Interne peut être utilisé pour signaler des comportements qui :

- **enfreignent la loi** (nationale, européenne ou internationale) ; ou
- **enfreignent notre code de conduite ou d'autres politiques de l'entreprise.**

Il ne peut pas être utilisé pour signaler un incident ou une plainte qui n'est pas lié à une violation d'une règle juridique ou à une violation d'une politique de l'entreprise, comme des questions individuelles liées à l'emploi, des suggestions d'amélioration de notre méthode de travail, des difficultés au sein d'une équipe ou des questions sur l'interprétation de nos politiques.

Le dispositif d'Alerte Interne n'est pas non plus destiné à signaler des situations dangereuses nécessitant une intervention urgente.

Pour aborder ces questions, vous devez utiliser d'autres canaux appropriés (tels que l'outil QHSE, votre superviseur, votre partenaire RH, ...).

Si vous n'êtes pas sûr qu'une question relève de la Politique Lanceur d'Alerte, vous pouvez demander conseil à nos référents Alerte.



## Comment signaler

---



Vous pouvez soumettre un signalement d'Alerte **en appelant nos référents Alerte ou en utilisant notre outil de signalement en ligne.**

- **Appel à nos référents Alerte**

Vous trouverez le numéro de téléphone des référents Alerte désignés pour chaque pays sur notre site web (sous la rubrique "ESG" > "Whistleblowing") et, pour les membres du personnel, également sur l'intranet de notre entreprise. Sélectionnez le pays auquel se rapporte votre signalement.

- **Notre outil de signalement en ligne**

Le lien vers l'outil est mentionné sur notre site web (dans la section "ESG" > "Whistleblowing") et, pour les membres du personnel, également sur l'intranet de notre entreprise.

Cet outil vous permet de soumettre un signalement par écrit ou par le biais d'un système d'enregistrement vocal. La page d'accueil de l'outil donne des conseils pratiques sur la manière de l'utiliser.

Lorsque vous soumettez un signalement en ligne, vous pouvez toujours **démander un entretien** avec un référents Alerte.



## Signalement anonyme

---

Notre dispositif d'Alerte Interne en ligne permet de soumettre des signalements de manière anonyme. Cela signifie que votre identité n'est connue ni de nous ni du fournisseur de l'outil.

Votre anonymat est garanti par plusieurs mesures :

- Aucun cookie ou suivi n'est appliqué sur la page de signalement. L'outil ne suit pas et ne stocke pas l'adresse IP ou l'ID machine de l'appareil utilisé pour le signalement.
- Les métadonnées (par exemple, les informations sur l'auteur d'un fichier, l'heure et le lieu de création du fichier) sont automatiquement supprimées de tous les fichiers que vous pouvez télécharger vers l'outil.
- Si vous choisissez de faire un signalement oral (via le système d'enregistrement vocal), l'outil peut déformer votre voix de manière à ce qu'elle ne soit pas reconnaissable.



## Traitement des signalements

---

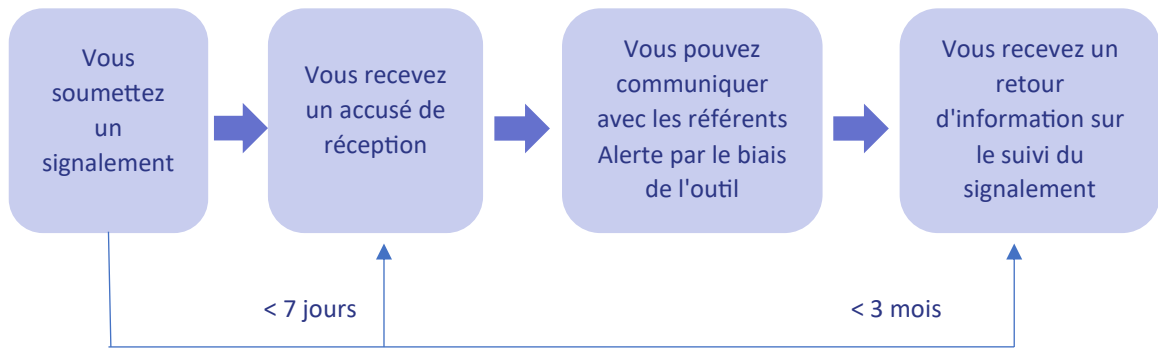


Tous les signalements sont **reçus (uniquement) par nos référents Alerte.**

Ces référents sont des membres du personnel d'Euroports qui ont été spécifiquement désignés et formés pour traiter les signalements de manière impartiale et confidentielle.

Les **sections spécifiques à chaque pays figurant à l'annexe A de la présente politique** décrivent qui sont les référents Alerte pour chaque pays dans lequel Euroports opère.

Si vous indiquez dans l'outil en ligne que votre signalement concerne le service dans lequel travaille l'un des référents Alerte, ce dernier ne recevra pas votre signalement et celui-ci sera uniquement envoyé aux autres référents Alerte, afin d'éviter tout conflit d'intérêts.



L'un des référents Alerte vous enverra un **accusé de réception** du signalement dans les 7 jours.

Si votre signalement est irrecevable (par exemple parce qu'il porte sur une question qui ne peut être signalée par le biais de la procédure de signalement), les référents Alerte vous en informeront, clôtureront le dossier et vous orienteront vers une autre voie appropriée.

Nous nous engageons à faire en sorte que **nos référents Alerte enquêtent de manière approfondie, objective et diligente sur chaque signalement recevable**.

Les référents Alerte peuvent faire appel à des experts internes et/ou externes pour les aider dans l'enquête et/ou le suivi du signalement (appelés dans le présent document "gestionnaires de dossiers désignés").

Il peut vous être demandé de fournir des éclaircissements ou des informations supplémentaires.

Vous recevrez un **code unique** qui vous permettra de vous connecter ultérieurement à l'outil, de vérifier le retour d'information des référents Alerte et de fournir des informations complémentaires.

- Si vous soumettez le signalement via l'outil en ligne, l'outil génère ce code unique. Il en va de même si vous choisissez de faire votre déclaration de manière anonyme.
- Si vous soumettez le signalement en appelant un référent Alerte, celui-ci créera un dossier dans l'outil et vous fournira le code unique.

Les référents Alerte conserveront des enregistrements appropriés de toutes les actions d'enquête. Dans tous les cas où les référents Alerte ou les gestionnaires de dossiers désignés établissent un procès-verbal ou une transcription d'une conversation orale, la personne interrogée a le droit de vérifier, de rectifier et d'accepter le procès-verbal/la transcription.

Les référents Alerte respecteront le droit à la défense de la personne signalée.

Dans les trois mois suivant l'accusé de réception, un référent Alerte vous **informera de la suite donnée à votre signalement**.

En fonction des résultats de l'enquête, Euroports prendra les **mesures de suivi appropriées**. Il peut s'agir, par exemple, de sanctions disciplinaires, de la cessation de la collaboration, de transmission de l'information à la police ou d'autres actions en justice.



## Confidentialité

---



### Tous les signalements sont traités de manière confidentielle.

Cet engagement de confidentialité concerne

- votre identité ;
- l'identité de la personne signalée et des autres personnes impliquées ; et
- les problèmes signalés.

Seuls les référents Alerte ont **accès** à votre signalement et aux données du dossier (qui sont stockées dans l'outil en ligne). Les référents Alerte n'ont accès qu'aux dossiers pour lesquels ils ont été désignés. Les référents Alerte peuvent donner accès aux gestionnaires de dossiers désignés sur la base du besoin de savoir.

Les référents Alerte ont pour instruction et formation de préserver la confidentialité de **l'identité du** Lanceur d'Alerte, de la personne signalée et des autres personnes impliquées, sauf dans les cas suivants :

- avec le consentement de la personne concernée ; ou
- lorsque nous sommes légalement tenus de divulguer l'identité dans le cadre d'enquêtes menées par une autorité ou de procédures judiciaires (dans ce cas, la personne concernée sera informée à l'avance, sauf si cela risque de compromettre l'enquête/la procédure).

Les référents Alerte ont reçu des instructions et une formation leur permettant de préserver la confidentialité des **problèmes signalés** et de ne les partager qu'avec d'autres personnes :

- sur la base d'une nécessité de connaissance, avec les gestionnaires de dossiers désignées ;
- avec notre direction (au cours de l'enquête, seules des données limitées sont partagées) ; ou
- avec les autorités ou d'autres parties externes, lorsque la loi l'exige ou lorsque l'intérêt public le justifie.

Toute divulgation visée ci-dessus est limitée aux données pertinentes au regard de l'objectif spécifique de la divulgation.

Les gestionnaires de dossiers désignées sont soumises aux mêmes obligations de confidentialité que les référents Alerte.

Si l'enquête conclut à l'existence d'une faute, les détails de la faute établie et l'identité des personnes responsables de la faute seront divulgués à la direction d'Euroports et aux services concernés (par exemple, les RH) et, le cas échéant, aux autorités ou à d'autres parties externes concernées.



## Sécurité

---

Des efforts considérables sont déployés pour sécuriser les données relatives au signalement. Le fournisseur de notre outil en ligne met fortement l'accent sur la sécurité, la confidentialité et la conformité au GDPR.

Notre fournisseur d'outils en ligne applique des mesures de sécurité technologique appropriées, notamment des pare-feu, des logiciels antivirus et un **cryptage de bout en bout**. Toutes les données relatives aux dossiers sont cryptées avant d'être stockées dans la base de données du fournisseur de l'outil. Nous sommes les seuls à recevoir les clés de décryptage.

Le fournisseur de l'outil est certifié ISO 27001 et fait l'objet d'audits et de tests de pénétration réguliers.





## Protection contre les représailles

---



**Euroports ne tolère aucune forme de représailles** à l'encontre des Lanceurs d'Alertes ou des personnes impliquées dans l'enquête ou le suivi d'un signalement.

Les représailles comprennent toute forme d'intimidation, de menace, de harcèlement, de sanction ou d'autre traitement défavorable. Par exemple, si vous êtes membre du personnel, vous ne ferez pas l'objet d'un licenciement, d'une sanction disciplinaire ou d'un autre traitement défavorable en raison du fait que vous avez soumis un signalement d'alerte en toute bonne foi.

En outre, dans certaines circonstances, vous pouvez bénéficier d'une protection juridique spécifique contre toute représailles prévue par la législation nationale en matière de signalement.

- Cette protection juridique s'applique généralement aussi aux personnes qui aident le Lanceur d'Alerte dans le cadre de la procédure de signalement et aux personnes qui ont un lien avec le Lanceur d'Alerte (par exemple, les membres de sa famille).
- Les sections spécifiques à chaque pays de l'annexe A de cette politique fournissent de plus amples informations sur les conditions à remplir pour bénéficier d'une telle protection juridique.

Nous prendrons des mesures disciplinaires ou autres à l'encontre des personnes qui agissent de mauvaise foi et **font sciemment un faux signalement**. Dans ce cas, d'autres sanctions légales (civiles ou pénales) peuvent s'appliquer, en fonction de la législation nationale.

De telles mesures ne seront pas prises à l'encontre des personnes qui, de bonne foi, font part de leurs soupçons, lorsque l'enquête conclut qu'aucune conduite illégale ou contraire à l'éthique n'a été commise.



## Protection des données personnelles

---

Le traitement des données à caractère personnel dans le cadre de la présente Politique Lanceur d'Alerte aura lieu conformément aux exigences du règlement général européen sur la protection des données (RGPD) et de toute législation locale en matière de protection des données (le cas échéant).

La **déclaration de confidentialité** figurant à l'**annexe B** de la présente politique fournit de plus amples informations à cet égard.



## Signalements externes

---

Nous vous encourageons vivement à signaler tout comportement illégal ou contraire à l'éthique *en interne*, soit de manière informelle, soit par l'intermédiaire de notre système de signalement interne. Cela nous permet d'enquêter efficacement et de prendre immédiatement les mesures qui s'imposent.

Au sein de l'UE, vous avez également le droit, dans certains cas, de signaler les infractions à l'*extérieur* aux autorités compétentes.

- Les sections spécifiques à chaque pays de l'annexe A de la présente politique contiennent de plus amples informations sur la communication externe aux autorités nationales compétentes.
- En outre, certains organes, bureaux et agences de l'Union européenne sont compétents pour recevoir des signalements d'alerte externe.<sup>1</sup>



## Modification de la présente politique

---

La présente politique, y compris ses annexes, sera revue et mise à jour périodiquement afin de garantir son efficacité et son alignement sur les normes juridiques, techniques et éthiques.



## Questions concernant cette politique

---

Si vous avez des questions concernant cette politique, vous pouvez **contacter les Référents Alerte désignés pour votre pays** (dont la liste figure dans l'annexe de cette politique consacrée au pays concerné et sur notre site web et notre intranet).

---

<sup>1</sup> Il s'agit, par exemple, de la [Commission européenne](#), de l'Office européen de lutte antifraude ([OLAF](#)), de l'Agence européenne pour la sécurité maritime ([AESM](#)), de l'Agence européenne de la sécurité aérienne ([AESA](#)), de l'Autorité européenne de sécurité et des marchés ([AESM](#)), de l'Agence européenne des médicaments ([EMA](#)) et du [Parquet européen](#).

## A. Annexes par pays



### FRANCE

#### Référents Alerte

Les référents Alerte nommés par les entités françaises du groupe Manuport Logistics sont :

- le Chief Corporate and Development Officer (Group Legal) ;
- le directeur général des ressources humaines (RH Groupe) ; et
- le responsable mondial des ressources humaines de MPL.

Les référents Alerte nommés par les autres entités françaises du groupe Euroports sont les suivants :

- le Chief Corporate and Development Officer (Group Legal) ; et
- le directeur général des ressources humaines (Group HR).

#### Législation nationale sur le lanceur d'alerte

La législation française mettant en œuvre la directive européenne 2019/1937 se compose des textes suivants :

- Articles 6 à 16 de la "*Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique*" (la "Loi Sapin II")  
(<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033558528>) ;
- "*Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte*"  
(<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000045388745>) ;
- "*Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte*"  
(<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000046357368>) ;
- Articles L. 1121-2 et L. 1132-3-3 du *Code du travail*  
([https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000045389811](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045389811)) et  
([https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000045391816](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045391816)) ;

	<ul style="list-style-type: none"><li>- Articles 122-9 et 225-1 du <i>Code pénal</i> (<a href="https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045391764">https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045391764</a> et <a href="https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045391831">https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045391831</a>).</li></ul> <p>(ci-après dénommée "la loi française sur le lanceur d'alerte").</p> <p>Vous pouvez consulter le texte de cette législation sur les sites web susmentionnés.</p>
Protection juridique	Les conditions pour bénéficier de la protection juridique contre les rétorsions sont énoncées aux articles L. 1121-2 et L. 1132-3-3 du <i>Code du travail</i> et aux articles 122-9 et 225-1 du <i>Code pénal</i> .
Signalements externes	<p>Vous pouvez faire part de vos préoccupations aux autorités compétentes lorsque la faute que vous souhaitez signaler concerne une violation des dispositions légales énumérées dans la loi française sur le lanceur d'alerte des dysfonctionnements. Cette liste figure à l'article 6 de la <i>loi Sapin II</i>.</p> <p>Vous pouvez trouver des informations sur les autorités françaises compétentes pour recevoir les signalements d'alerte externe et sur la manière de déposer un tel signalement sur le site web du gouvernement suivant : <a href="https://www.service-public.fr/particuliers/vosdroits/F32031">https://www.service-public.fr/particuliers/vosdroits/F32031</a>.</p>

*Les annexes des autres pays sont incluses dans la politique du groupe (publiée sur l'intranet et le site web du groupe).*

## B. Déclaration de confidentialité

La présente déclaration de confidentialité explique comment et pourquoi les données à caractère personnel sont traitées dans le cadre de la Politique Lanceur d'Alerte d'Euroports, comment nous les protégeons, combien de temps nous les conservons et qui vous pouvez contacter.

Aux fins de la présente déclaration de confidentialité relative au lanceur d'Alerte, le terme "vous" désigne chacune des personnes concernées décrites ci-dessous.

Tous les traitements sont effectués en conformité avec le règlement général européen sur la protection des données (RGPD) et les réglementations locales en matière de protection des données (le cas échéant).

### *Finalité du traitement*

La procédure de signalement vise à fournir un canal par lequel les préoccupations concernant les violations du droit (national, européen ou international) au sein de l'organisation Euroports et les violations du code de conduite d'Euroports ou d'autres politiques peuvent être signalées, afin qu'elles puissent faire l'objet d'une enquête et que des mesures appropriées puissent être prises.

L'objectif ultime est de promouvoir une culture d'entreprise où des comportements fautifs ne sont pas tolérés et d'accroître la transparence et l'intégrité au sein du groupe Euroports. La mise en place d'un dispositif d'Alerte Interne sûr, confidentiel et anonyme est considérée comme un élément essentiel d'une politique efficace en matière d'intégrité et de conformité.

### *Champ d'application du traitement*

Toutes les entités du groupe Euroports agissent en tant que responsables du traitement des données à caractère personnel dans le cadre de leur Politique Lanceur d'Alerte, conformément aux accords conclus au sein du groupe.

Les personnes concernées sont

- les Lanceur d'Alertes mentionnés dans la section "*Champ d'application*" de notre Politique Lanceur d'Alerte ;
- les personnes mentionnées dans un signalement d'alerte ou dans l'enquête connexe ; et
- les témoins et les autres personnes qui fournissent des informations dans le cadre de l'enquête.

La personne signalée est informée du signalement dès que cela est raisonnablement possible. Cette information sera retardée et/ou son contenu sera limité s'il existe un risque d'entrave à l'enquête ou à la collecte de preuves ou de divulgation de l'identité du Lanceur d'Alerte.

Aucune prise de décision automatisée n'est appliquée, ce qui signifie que nous ne fondons aucune décision vous concernant sur le seul traitement automatisé de vos données à caractère personnel.

### ***Données traitées***

Les données à caractère personnel traitées sont recueillies auprès du Lanceur d'Alerte, de la personne signalée, des témoins et d'autres personnes susceptibles d'être impliquées dans l'affaire ou d'apporter des éclaircissements.

Les données peuvent comprendre les éléments suivants :

- les données d'identification ;
- les problèmes signalés ;
- les informations obtenues dans le cadre de l'enquête ;
- des informations sur les résultats de l'enquête et sur les éventuelles mesures de suivi prises.

Les données peuvent éventuellement comprendre :

- les données judiciaires ou pénales (par exemple, en cas de préoccupations susceptibles de constituer une infraction pénale) ;
- des données à caractère personnel sensibles (c'est-à-dire des catégories particulières de données à caractère personnel qui révèlent l'appartenance syndicale, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ...). En principe, ce ne sera pas le cas, car Euroports n'a pas l'intention de traiter de telles données et l'outil ne comporte pas de questions à ce sujet. Toutefois, étant donné le large éventail de sujets auxquels le signalement peut se référer, il est possible que le signalement contienne de telles données.

### ***Motifs juridiques du traitement***

Le traitement est nécessaire :

- pour se conformer à une obligation légale à laquelle Euroports est soumis (sur la base de la directive 2019/1937 de l'UE sur la protection des personnes qui signalent des violations du droit de l'Union et de la législation nationale de mise en œuvre mentionnée dans les annexes nationales de notre Politique Lanceur d'Alerte) ; et
- aux fins des intérêts légitimes poursuivis par Euroports (tels qu'expliqués ci-dessus dans la section "*Finalité du traitement*").

### ***Destinataires des données et sous-traitants***

L'accès aux données personnelles est limité comme indiqué dans la section "*Confidentialité*" de notre Politique Lanceur d'Alerte.

Le fournisseur de notre outil de signalement en ligne (Whistleblower Software ApS) est un sous-traitant.

### ***Protection des données***

Les données à caractère personnel sont protégées comme indiqué dans les sections "*Sécurité*" et "*Confidentialité*" de notre Politique Lanceur d'Alerte.

### ***Transfert de données***

En principe, il n'y aura pas de transfert de données à caractère personnel concernant des personnes de l'Espace économique européen ("EEE") à des destinataires situés en dehors de l'EEE. Les serveurs de notre fournisseur d'outils en ligne sont situés dans l'Union européenne.

Toutefois, dans certaines circonstances, les données peuvent être partagées avec des destinataires situés dans des pays n'appartenant pas à l'EEE sur la base d'un strict besoin d'en connaître (par exemple, si le signalement concerne une faute présumée commise par des personnes situées dans des entités du groupe à la fois dans l'EEE et en dehors de l'EEE). Si, dans ce cas, il n'y a pas de décision d'adéquation concernant le pays non-membre de l'EEE concerné, Euroports veille à l'application de garanties appropriées, telles que les clauses types de la Commission européenne.

### *Conservation des données*

Vos données personnelles seront conservées pendant une durée n'excédant pas celle nécessaire et proportionnée, en tenant compte des facteurs suivants :

- toute exigence légale concernant la conservation des données ;
- le type de signalement (irrecevable, pas de faute établie, faute établie) ;
- le délai de prescription pendant lequel l'enquête et les mesures de suivi d'Euroports peuvent être contestées ; et
- tout lien avec des procédures disciplinaires ou judiciaires, des enquêtes criminelles ou d'autres enquêtes ou procédures menées par une autorité.

### *Personne de contact et droits de la personne concernée*

Si vous avez des questions concernant le traitement de vos données personnelles, vous pouvez contacter les référents Alerte désignés pour votre pays (dont la liste figure dans l'annexe nationale de notre Politique Lanceur d'Alerte et sur notre intranet et notre site web (sous la rubrique "ESG" > "Whistleblowing")).

Vos droits en tant que personne concernée sont expliqués dans notre déclaration de confidentialité générale GDPR, qui peut être consultée sur notre [site web](#).

Les demandes d'exercice de vos droits de personne concernée en vertu de la présente déclaration de confidentialité relative au signalement doivent (par dérogation à la section 5.2 de notre déclaration de confidentialité générale relative au GDPR) être envoyées à l'adresse suivante : [whistleblowing@euroports.com](mailto:whistleblowing@euroports.com). Ce compte de messagerie est géré par les référents Alerte du groupe (Group Legal et Group HR) afin de garantir la confidentialité. Les Lanceurs d'Alertes peuvent également choisir d'envoyer une demande concernant leurs droits en tant que personne concernée en se connectant à l'outil en ligne à l'aide de leur code unique.

Nom du document :	Politique Lanceur d'Alerte
Propriétaire :	Groupe RH
Réциpiendaires :	Tous les membres du personnel du groupe Euroports (y compris les employés et les consultants (de projet)) + toutes les autres personnes ayant une relation professionnelle actuelle, passée ou future avec Euroports (clients, fournisseurs, candidats à l'emploi, anciens membres du personnel, ...).
Version :	Version 1
Date :	20-12-2023
Approbation :	Comité exécutif du groupe
Nom du fichier :	FR_Politique Lanceur d'Alerte France_Whistleblowing policy
Une mise en œuvre au niveau national est-elle nécessaire ?	<input checked="" type="checkbox"/> Oui, selon la <input checked="" type="checkbox"/> politique ; <input type="checkbox"/> Instruction de travail <input type="checkbox"/> Non
Une mise en œuvre au niveau du terminal est-elle nécessaire ?	<input checked="" type="checkbox"/> Oui, selon la <input checked="" type="checkbox"/> politique ; <input type="checkbox"/> Instruction de travail <input type="checkbox"/> Non
Une traduction au niveau national est-elle nécessaire ?	<input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non
À mettre en œuvre par	Responsable RH pays
<i>Cette politique est publique (à usage interne et externe) et peut être divulguée à des tiers.</i>	