Corporate Directive	Dispositif d'Alerte	UPSA-CORP-DIR-HQ-007
		Version 6

Historique des changements

Version	Date d'effet	Description des modifications
1	10 décembre 2019	Première version.
2	10 août 2021	> Exigence 3 : ajout de la ligne d'alerte interne dédiée à UPSA Italie > Exigence 6 : précisions sur l'évaluation du dispositif de ligne d'alerte interne > Changement du format pour alignement sur le format « Qualité »
3	11 décembre 2021	> Remplacement de la ligne d'alerte interne France par la nouvelle ligne d'alerte interne du Groupe Taisho > Ajout du process relatif aux référents harcèlement CSE (France) > Mise à jour des Exigences en conséquence
4	*Cf. date CARA*	Modification du Champ d'application et des Exigences 1, 3 et 4 suite aux nouvelles lois françaises sur la protection des lanceurs d'alerte, liées à la directive européenne (UE) n°2019/1937 du 23 octobre 2019
5	*Cf. date CARA*	> Reprise des éléments du document « Note relative à la confidentialité de la ligne d'alerte compliance Taisho » pour les intégrer au sein de la présente Directive et avoir document unique > Précisions apportées au sein des Exigences 1, 2, 3, 5 et 6 pour améliorer la clarté des informations apportées > Modifications apportées à l'Exigence 4 et à l'Annexe 1 à la suite de la mise-à-jour du process de gestion des alertes internes au sein du Groupe UPSA et du Groupe Taisho
6	*Cf. date CARA*	Modifications apportées à la procédure à la suite du changement de l'outil utilisé dans le Groupe pour la gestion du dispositif d'alerte interne (l'outil TSUHO est remplacé par l'outil DQ Helpline)

Objet

Préciser le cadre des alertes et signalements, le processus associé et les garanties permettant la protection des auteurs de tels alertes ou signalements.

Sommaire

Champ d'application

Dans le champ d'application
Qui est concerné par cette directive ? Cette directive s'applique à tous les employés actuels et passés d'UPSA ainsi qu'au personnel externe (intermédiaires, consultants, prestataires de services), au personnel temporaire (employés de prestataires de services avec lesquels UPSA travaille occasionnellement) et aux candidats à un emploi chez UPSA. Elle s'applique également à tous les employés actuels et passés de tout tiers d'UPSA (fournisseurs, clients...).

Références

- [Loi française] « Loi Sapin 2 » - Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique
- Directive européenne (UE) n°2019/1937 du 23 octobre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union Européenne
- [Loi française] Loi organique n°2022-400 du 21 mars 2022 visant à renforcer le rôle du Défenseur des droits en matière de signalement d'alerte, entrée en vigueur le 23 mars 2022.
- [Loi française] Loi ordinaire n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, en vigueur le 1er septembre 2022.
- « Loi 231 » applicable en Italie - Decreto legislativo 8 giugno 2001, n. 231
- Directive Globale relative à la Conformité du Groupe Taisho

Exigences

UPSA utilise le dispositif d'alerte mis en place par le Groupe Taisho. Pour signaler des actes ou des faits inappropriés, vous pouvez accéder à la ligne d'alerte de Taisho en vous connectant sur le site web suivant : **https://i365.dqhelpline.com/taishopharma/upsa07509**

Utilisez l'identifiant et le mot de passe communs ci-dessous pour vous connecter et soumettre votre alerte (Voir Annexe 1) :

- Identifiant : **alertUPSA**
- Mot de passe : **UPSA39466**

Pour l'Italie spécifiquement, la Loi 231 requiert une ligne d'alerte spécifique. Vous pouvez utiliser l'adresse e-mail suivante pour émettre une alerte : complianceitaly@upsa-ph.com

Exigence 1 : Définition d'un lanceur d'alerte

- Le lanceur d'alerte est une personne physique qui :
  - a personnellement eu connaissance des faits qu'il rapporte, ou a obtenu des informations dans le cadre de ses activités professionnelles (y compris s'il n'est pas ou plus salarié de UPSA : candidat non retenu, salarié dont la relation de travail avec UPSA s'est terminée, ou salarié d'une entreprise en contrat avec UPSA) ;
  - agit de manière désintéressée, sans contrepartie financière directe, pour son action ;
  - agit de bonne foi : au moment où il émet son alerte, les faits rapportés doivent présenter toutes les apparences d'un acte inapproprié, de sorte que le dénonciateur ne puisse être accusé d'avoir cherché à nuire à autrui.

Exigence 2 : Les faits pouvant donner lieu à un signalement

- Les informations révélées portent sur des faits qui se sont produits ou qui sont très susceptibles de se produire au sein du Groupe. Ces informations peuvent concerner :
  - Un crime ou un délit ;

- La violation ou la tentative de dissimulation de violation d'une loi ou d'un règlement, y compris du droit international ou de l'Union européenne ;
- La violation d'un acte juridique national ou international ;
- Une menace ou un préjudice pour l'intérêt général ;
- Une violation de la Directive Globale relative à la Conformité du Groupe Taisho ou des situations / comportements susceptibles de constituer des atteintes aux règles de probité définies par le Groupe.

Plus précisément, les faits pouvant être signalés peuvent se rapporter aux domaines suivants :

1. Sujets relatifs à la comptabilité ou aux audits
2. Situations de corruption ou pot-de-vin
3. Violation de la législation anti-trust
4. Conflit d'intérêts
5. Discrimination ; harcèlement (sexiste / sexuel / moral)
6. Détournement de fonds ; fraude
7. Violation des lois sur la protection de l'environnement, de la santé ou de la sécurité de l'environnement
8. Falsification ou altération de contrats, rapports ou registres
9. Falsification ou détournement de données
10. Délit d'initié
11. Actes de sabotage ou de destruction
12. Vol
13. Agression, intimidation
14. Comportement qui viole la protection des dénonciateurs, des individus coopérants et la protection des informations personnelles
15. Violation du Code de conduite du Groupe
16. Violation des règles et procédures internes qui conduisent à l'une des conduites énumérées ci-dessus

- Le signalement doit fournir les faits, informations, documents, de nature à étayer son contenu.
- Une information confidentielle peut faire l'objet d'un signalement sous réserve de respecter les contraintes légales (par ex : article 122-9 du Code Pénal Français). L'alerte ne peut pas porter sur des éléments couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client.

Exigence 3 : Le lanceur d'alerte bénéficie de garanties et d'une protection particulière

Protection du lanceur d'alerte

- Le lanceur d'alerte bénéficie des garanties suivantes :

- Une irresponsabilité civile concernant les dommages qui seraient causés du fait de l'alerte, sous réserve de respecter les conditions cumulatives suivantes :
  - Le lanceur d'alerte répond aux critères de définition du lanceur d'alerte ;
  - Le lanceur d'alerte avait des motifs raisonnables de croire que l'alerte était nécessaire à la sauvegarde des intérêts en cause.
- Une immunité pénale :
  - lorsque l'alerte porte atteinte à un secret protégé par la loi ; et
  - lorsque cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause ; et
  - lorsque qu'elle intervient dans le respect des procédures de signalement définies par la loi ; et
  - lorsque l'auteur de l'alerte répond aux critères de définition du lanceur d'alerte.

- L'absence de sanction disciplinaire ou de toute mesure de représailles en lien avec l'alerte, sous réserve d'une alerte de bonne foi et désintéressée, même si les faits s'avèrent finalement inexacts ou ne donnent lieu à aucune suite.
- Les éléments de nature à identifier l'émetteur de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec son consentement.
- Lorsque les personnes chargées du recueil et du traitement des alertes au sein du Groupe sont tenues de dénoncer les faits à l'autorité judiciaire, les éléments de nature à identifier l'auteur de l'alerte pourront être communiqués à cette dernière. Dans ce cas, l'auteur de l'alerte en sera informé, à moins que cette information ne risque de compromettre la procédure judiciaire.
- La personne qui fait l'objet d'une alerte ne peut en aucun cas obtenir communication des informations concernant l'identité de l'émetteur de l'alerte.

o Les mêmes garanties s'appliquent aux facilitateurs, c'est-à-dire toute personne physique ou morale de droit privé à but non lucratif ayant aidé le lanceur d'alerte à signaler et divulguer des informations relatives aux faits dénoncés (associations, syndicats, etc.).

o Toutefois, ces mesures de protection ne sont pas applicables si le lanceur d'alerte ne respecte pas les Exigences 1 et 2. Les lanceurs d'alerte de mauvaise foi (c'est-à-dire en connaissance de la nature fausse des faits dénoncés) peuvent :

- perdre le bénéfice de la protection et faire l'objet d'une sanction disciplinaire pouvant aller jusqu'au licenciement pour faute grave ou lourde en présence d'une intention de nuire ;
- être poursuivi pour dénonciation calomnieuse (par exemple, dans le cadre de la loi Sapin 2 : peine potentielle de 5 ans d'emprisonnement et 45 000 € d'amende (C. pén., art. 226-10)) ;
- être déclaré civilement responsable et condamné à verser des dommages et intérêts pour indemniser la victime.

<u>Confidentialité du lanceur d'alerte</u>

- L'identité de l'émetteur d'une alerte, des personnes visées par l'alerte, de tout tiers qui y est mentionné, ainsi que l'ensemble des informations recueillies dans le cadre du présent dispositif sont traitées de façon confidentielle.
- La gestion de l'alerte ne s'appuie que sur des données formulées de manière objective et faisant apparaître le caractère présumé des faits signalés. Seules les données en rapport direct avec le périmètre décrit dans l'Exigence 2 et strictement nécessaires à la vérification des faits allégués sont recueillies. Les données relatives à l'émetteur de l'alerte, aux personnes faisant l'objet d'une alerte et aux personnes intervenant dans le recueil ou le traitement de l'alerte sont limitées à leur identité, leurs fonctions et leurs coordonnées. Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.
- Les personnes chargées du recueil et du traitement des alertes sont en nombre limité, et sont astreintes à une obligation renforcée de confidentialité définie contractuellement. Elles n'accèdent à tout ou partie des données traitées que dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions et dans la limite de leurs attributions respectives.
- Des mesures appropriées sont prises pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur communication ou de leur conservation.
- Pour information, selon la loi Sapin 2, la divulgation d'informations confidentielles est punie de 2 ans d'emprisonnement et de 30 000 € d'amende.

<u>Protection des données</u>

- ***<u>Vos droits :</u>*** En application du Règlement Général sur la Protection des Données n°2016/679 du 27 avril 2016 (« RGPD ») et de la loi « Informatique et Libertés » du 6 janvier 1978 modifiée, chaque personne dispose d'un droit d'accès à ses données ainsi que le droit de se les faire communiquer, d'un droit

d'opposition et de limitation du traitement, et de demander à ce que ses données soient rectifiées, complétées et/ou effacées. Afin d'exercer vos droits en matière de protection des données ou pour toute question, veuillez contacter le Délégué à la Protection des Données d'UPSA à l'adresse suivante : EUDPO@upsa-ph.com.

- ***Mesures de protection des données :*** En ce qui concerne le dispositif d'alerte de Taisho, le Groupe prend les mesures appropriées pour préserver la confidentialité et la sécurité des données traitées dans le cadre de l'alerte, en application des dispositions du RGPD et de la Loi informatique et libertés.
- ***Données personnelles utilisées :*** Lors de l'utilisation de la ligne d'alerte, des données personnelles peuvent être fournies par le lanceur d'alerte, par des personnes autorisées participant à l'enquête, ou par des personnes interrogées au cours de l'enquête. Selon le contenu de l'alerte, les catégories de données suivantes sont traitées :
    - si le lanceur d'alerte décide de ne pas rester anonyme, le nom et l'adresse e-mail de ce dernier, ainsi que le nom de la société à laquelle il appartient et le pays de son lieu de travail ;
    - l'identité des personnes visées par l'alerte ou de tout tiers qui y est mentionné ;
    - les événements rapportés dans l'alerte et les informations connexes ;
    - les informations recueillies au cours de l'enquête et formalisées au sein du rapport d'enquête ;
    - Les mesures prises en réponse l'enquête ;
    - En fonction du contenu de l'alerte, et uniquement si cela s'avère nécessaire, les personnes chargées du recueil et du traitement des alertes au sein du Groupe peuvent être amenées à traiter des données personnelles sensibles au sens du RGPD (telles que des données de santé, des données révélant l'origine raciale ou ethnique, des données sur la vie sexuelle ou l'orientation sexuelle d'une personne, etc.).

  Le lanceur d'alerte est invité à remonter uniquement des informations factuelles et présentant un lien direct avec l'objet de l'alerte dans le cadre du signalement.

- ***Destinataires des données personnelles et anonymat :***
    - Pour une information relative aux destinataires des données, veuillez-vous reporter aux Exigences 4 et 5 de la présente Directive.
    - Le dispositif permet au lanceur d'alerte de rester anonyme s'il le souhaite, tout en lui permettant de suivre son signalement à l'aide du code unique qui lui est remis lors de l'envoi de son signalement (ce code permet au lanceur d'alerte, même s'il est anonyme, de vérifier si des

réponses, des mises-à-jour ou des demandes de fournir des détails ou des informations complémentaires ont été apportées à son signalement).

- ***Finalités et bases juridiques liées à l'utilisation des données personnelles :***
  - Les traitements ont pour finalité le signalement et le traitement des alertes, incluant la réalisation d'enquêtes sur les faits signalés, relatives aux actes mentionnés au sein de l'Exigence 2 de la présente Directive. Seules les données nécessaires à la gestion de l'alerte peuvent être traitées par le Groupe.
  - Les traitements mis en œuvre ont pour base légale :
    - le consentement du lanceur d'alerte en application de l'article 6§1 a) du RGPD ;
    - le respect des obligations légales auxquelles le Groupe est soumis en application de l'article 6§1 c) du RGPD, en particulier les législations listées au début de la présente Directive ;
    - L'intérêt légitime poursuivi par le Groupe Taisho à travers la réalisation d'enquêtes visant des situations et des actes contraires au Code de Conduite du Groupe, en application l'article 6§1 f) du RGPD ;
    - A noter, que les données sensibles entrant dans le champ d'application de l'article 9 du RGPD ne seront traitées que : sur la base du consentement de la personne concernée (en application l'article 9§2 a) du RGPD), ou si elles sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice (en application de l'article 9§2 f) du RGPD).

- ***Transfert des données personnelles à l'étranger :*** La réalisation de ces finalités implique des transferts de données personnelles au Japon, puisque le département des Affaires Internes de Taisho est situé au Japon et que l'administrateur de la ligne d'alerte (DQ Helpline) est également situé au Japon. La conformité de ces transferts de données aux exigences des articles 44 et suivants du RGPD est garantie par la décision d'adéquation C/2019/304 de la Commission européenne, qui constate que le Japon assure un niveau de protection adéquat au sens de l'article 45 du RGPD.

  Pour la réalisation des enquêtes, tout autre transfert de données personnelles qui serait susceptible de se produire sera réalisé conformément aux articles 44 et suivants du RGPD et au droit applicable. De plus amples informations peuvent être demandées à l'adresse EUDPO@upsa-ph.com.

- ***Durée de conservation des données personnelles :***
    - Les données relatives aux signalements ne seront conservées que le temps strictement nécessaire à leur traitement.
    - Lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les données relatives à cette alerte sont détruites ou archivées après anonymisation, dans un délai de trente (30) jours à compter de la clôture des opérations de vérification.
    - Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont conservées jusqu'au terme de la procédure. Les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses (fin de délai de prescription).

Tout manquement à ces exigences expose l'auteur à d'éventuelles mesures disciplinaires ou poursuites judiciaires.

Exigence 4 : Le processus à respecter en cas de signalement

- Chaque collaborateur reste libre d'utiliser la ligne d'alerte ou de remonter une situation, une interrogation ou une difficulté par les voies alternatives suivantes :
    - via le système d'alerte interne du Groupe Taisho, via le site web suivant **https://i365.dqhelpline.com/taishopharma/upsa07509** en utilisant l'identifiant et le mot de passe communs ci-dessous :
        - Identifiant : **alertUPSA**
        - Mot de passe : **UPSA39466** ; ou
    - au supérieur hiérarchique direct ou indirect (pour les collaborateurs UPSA) ; ou
    - pour des faits particuliers relatifs à l'entité juridique UPSA Italie, aux membres du Supervisory Body italien : complianceitaly@upsa-ph.com; ou
    - pour les cas spécifiques liés au harcèlement dans l'entité juridique UPSA France, aux référents harcèlement désignés au sein des comités d'entreprise français de Rueil ou d'Agen (pour toute question sur ce dispositif, veuillez contacter le Département des Ressources Humaines) ; ou

- à la Direction Juridique et Compliance ;
- à la Direction des Ressources Humaines ;
- auprès des autorités compétentes externes à UPSA (notamment le Défenseur des droits).

- Le système d'alerte interne du Groupe Taisho est disponible 24h/24 et 7j/7 en plusieurs langues (dont le français, l'anglais, l'italien et l'espagnol).
- Les étapes du dispositif d'alerte du Groupe Taisho sont détaillées dans l'Annexe 1. Afin d'assurer à chaque lanceur d'alerte les garanties nécessaires au traitement équitable de son alerte, ce système est géré par le Département des Affaires Internes de Taisho (qui est le département en charge du siège social de Taisho Pharmaceuticals) via une société externe et indépendante, DQ Helpline. Il vous permet de signaler des faits afin que des investigations soient menées de manière confidentielle et impartiale par les personnes en charge du dispositif d'alerte au sein de ce Département du Groupe Taisho et le, cas échéant selon le contenu de l'alerte, de la Direction Juridique et Compliance d'UPSA ou de la Direction des Ressources Humaines d'UPSA.
- L'auteur de l'alerte peut, s'il le souhaite, s'identifier et son identité est traitée de façon confidentielle.
- Par exception, l'alerte formulée par une personne souhaitant rester anonyme peut être traitée sous les conditions suivantes :
  - La gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ;
  - Le traitement de cette alerte doit s'entourer de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif.
  - Dans le cas d'une alerte anonyme, l'auteur de l'alerte, doit être conscient que l'alerte puisse ne pas être traitée si elle ne répond pas aux conditions listées ci-dessus.

- L'auteur de l'alerte peut transmettre tout élément, quel que soit sa forme ou son support, de nature à étayer les faits objets de son signalement.

Exigence 5 : Le processus de traitement

- L'auteur de l'alerte reçoit un code unique lors de l'envoi de son signalement qui lui permet de retrouver les éléments qu'il a communiqués, mais également de vérifier si des réponses, des mises-à-jour ou des

demandes de fournir des détails ou des informations complémentaires ont été apportées à son signalement.

- L'auteur de l'alerte pourra être invité à fournir toute information complémentaire, permettant de vérifier les conditions de recevabilité de son signalement ou l'exactitude des faits dénoncés.
- L'auteur de l'alerte est informé des mesures envisagées ou prises, le cas échéant, dans un délai de 3 mois suivant l'accusé de réception de son alerte.
- La ou les personnes faisant l'objet de l'alerte sont informées du signalement. Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information peut être réalisée après l'adoption de ces mesures.
- La gestion de l'alerte, en particulier les opérations de vérification, est confiée à la personne la plus compétente dans le domaine concerné par le signalement au sein de la Direction des Ressources Humaines ou de la Direction Juridique et Compliance.
- L'instance Dirigeante UPSA est informée des situations les plus sensibles (sauf lorsqu'elle est mise en cause ou susceptible de l'être).
- Pour la réalisation des enquêtes, les informations recueillies par le biais de l'alerte peuvent être divulguées à des experts (tels que par exemple dans le domaine financier, comptable, informatique, ou juridique), aux autorités policières ou gouvernementales, si nécessaire pour se conformer aux exigences légales ou dans le cadre d'une action en justice, ainsi qu'à d'autres destinataires légitimes, lorsque la loi l'exige ou en relation avec toute procédure judiciaire.

  Le nombre de personnes participant à une enquête sera limité dans la mesure où cela est compatible avec une enquête pleine et entière et en conformité avec la législation applicable

- Au cours de l'enquête, dans la mesure où cela est nécessaire pour remédier et/ou sanctionner la faute établie, le ou les responsables hiérarchiques des personnes concernées par l'alerte en seront informés, en fonction de la gravité et de la nature des faits.
- L'auteur de l'alerte est informé des suites qui lui sont données par le système d'alerte, le Responsable Compliance ou le Responsable des Ressources Humaines en fonction des cas. Lorsque l'alerte est jugée irrecevable, l'auteur de l'alerte est informé des raisons de cette irrecevabilité.
- L'auteur de l'alerte et les personnes visées par celui-ci sont informés de la clôture de l'alerte.

Exigence 6 : Autres principes généraux à l'attention des utilisateurs du dispositif

- Le présent dispositif d'alerte revêt un caractère facultatif et sa non-utilisation n'entraîne aucune conséquence à l'égard des employés.

- Une utilisation abusive du dispositif expose son auteur à d'éventuelles sanctions ou poursuites.
- La qualité et l'efficacité de ce dispositif d'alerte sont évaluées a minima annuellement par le Département des Affaires Internes de Taisho et le Département Juridique et Compliance d'UPSA, aux travers d'indicateurs (notamment : nombre d'alertes reçues, classées sans suite ou traitées, délais de traitement, problématiques soulevées). Ces indicateurs sont partagés avec la Direction Générale d'UPSA périodiquement.
- Une copie de la présente directive est remise à chaque utilisateur potentiel du dispositif d'alerte (membres du personnel, collaborateurs extérieurs et occasionnels). Une copie de la présente directive est également remise à toute personne faisant l'objet d'une alerte, sauf si elle en a déjà reçu une copie au préalable.
- L'auteur de l'alerte peut choisir d'adresser son signalement, directement ou après avoir effectué un signalement interne, à l'une des autorités externes compétentes suivantes :
  - à l'une des autorités listées en annexe du décret n° 2022-1284 du 3 octobre2022, en fonction de l'objet de l'alerte ;
  - En France, au Défenseur des droits qui sera chargé d'orienter l'auteur de l'alerte vers la ou les autorités les mieux à même d'en connaitre, sauf dans le cas où il serait lui-même désigné comme étant l'autorité compétente ;
  - à l'autorité judiciaire ;
  - à une institution, un organe ou un organisme de l'Union européenne compétent pour recueillir des informations sur des violations entrant dans le champ matériel d'application de la directive (UE) 2019/1937 du 23 octobre 2019.

Rôles et Responsabilités

Voir les Exigences.

Définitions

N/A

Documents liés

N/A

Contact

Pour toute question sur ce document, adressez-vous au Département Legal & Compliance.

ANNEXE 1 – Description du système d'alerte de Taisho