Paradigm

Politique de protection des lanceurs d'alerte

Objectif et mission de Paradigm

Paradigm est un organisme d'intérêt public de catégorie A dont la mission est de préparer, gérer et implémenter la stratégie numérique de la Région Bruxelles-Capitale en veillant à l'accessibilité des usagers dans la réalisation de ses actions.

Paradigm met par la présente, son engagement en matière de protection des lanceurs d'alerte en conformité avec la directive de l'Union Européenne 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union européenne et ses textes de transposition en droit belge[1].

Paradigm adopte ainsi la présente politique de protection des lanceurs d'alerte. Ce document définit la procédure interne à suivre pour signaler une violation relevant du champ d'application des textes précités, la manière dont le signalement sera traité, et la protection accordée aux lanceurs d'alerte et aux personnes visées dans le cadre des signalements internes.

I. Qui peut effectuer un signalement ?

Au sein de Paradigm, peut effectuer un signalement ou lancer une alerte dans le cadre de la présente Politique **toute personne qui rapporte des informations sur des infractions dont elle a eu connaissance dans un contexte professionnel**.

Il en va ainsi de toutes les personnes qui ont une relation professionnelle avec Paradigm, y compris (liste non limitative) :

- Employés sous contrat à durée déterminée ou indéterminée et anciens employés ;
- Travailleurs indépendants et ex-travailleurs indépendants ;
- Constultants et ex-consultants ;
- Actionnaires, dirigeants et tous membres d'un organe d'administration, de direction ou de surveillance;
- Délégués syndicaux ;
- Bénévoles et stagiaires, rémunérés ou non ;
- Toute personne travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs de Paradigm;

---

[1] *Les décret et ordonnance conjoints des 26 avril et 16 mai 2019 relatifs au médiateur bruxellois tels que modifiés par les décret et ordonnance conjoints du 27 avril 2023 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, accompagnés de l'Arrêté du Gouvernement de la Région de Bruxelles-Capitale du 7 décembre 2023 portant exécution de l'article 15, §2 des décret et ordonnance conjoints de 2019 précité, ces textes transposant partiellement la directive de l'Union Européenne 2019/1937 du 23 octobre 2019.*

- **Candidat à l'embauche** dans le cas où des informations sur des infractions ont été obtenues au cours de la procédure de recrutement ou d'autres négociations précontractuelles.

II. Quelles violations peuvent être signalées ?

Peuvent être signalées :

1° les violations portées aux normes régissants les domaines suivants :

1. marchés publics ;
2. services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme ;
3. sécurité et conformité des produits ;
4. sûreté et sécurité de tous les moyens de transport ;
5. protection de l'environnement ;
6. radioprotection et sécurité nucléaire ;
7. sécurité des aliments destines à l'alimentation humaine et animale, santé et bien-être des animaux ;
8. santé publique ;
9. protection des consommateurs ;
10. protection de la vie privée et des données personnelles, et sécurité des réseaux et des systèmes d'information ;
11. entraves à la lutte contre la fraude fiscale ;
12. entraves à la lutte contre la fraude sociale.

2° les violations portant atteinte aux intérêts financiers de l'Union visés à l'article 325 du Traité sur le fonctionnement de l'Union européenne et précisés dans les mesures pertinentes de l'Union et, le cas échéant, dans les dispositions nationales d'implémentation;

3° les violations relatives au marché intérieur visé à l'article 26, paragraphe 2, du Traité sur le fonctionnement de l'Union européenne, y compris les violations des règles de l'Union en matière de concurrence et d'aides d'Etat.

Ainsi, peut être signalée toute atteinte ou suspicion d'atteinte à l'intégrité dans les domaines susvisés, à savoir tout acte ou omission qui est illicite ou qui va à l'encontre de l'objet ou de la finalité de toute norme juridique (dispositions européennes directement applicables, lois, ordonnances, décrets, arrêtés, circulaires, règlements, règles internes et procédures internes) et qui constitue une menace pour l'intérêt général ou une atteinte à celui-ci.

Signalements ne relevant pas de la présente politique :

Sont exclus de la catégorie des atteintes à l'intégrité visées par la législation protectrice des lanceurs d'alerte et ne sont pas protégés par la présente politique :

- le harcèlement moral, la violence au travail et le harcèlement sexuel au travail ; et
- la discrimination, directe ou indirecte (fondée sur l'âge, l'orientation sexuelle, l'état civil, la naissance, la fortune, les convictions religieuses, philosophiques, politiques ou syndicales, la langue, l'état de santé actuel ou futur, un handicap, une caractéristique physique ou génétique, le sexe, la grossesse, l'accouchement, la maternité, le changement de sexe, la nationalité, une prétendue race, la couleur de peau, l'ascendance, l'origine nationale, ethnique ou sociale).

La présente politique ne couvre pas non plus les plaintes relatives à l'emploi ou les griefs interpersonnels entre l'auteur du signalement et un.e autre collègue.

Il existe des procedures et des organes de protection spécifiques pour ces catégories de singalements.

III. Comment signaler une atteinte à l'intégrité à travers le canal interne de Paragidm ?

Le signalement peut être effectué à travers les différents moyens conçus, établis et gérés en interne, d'une manière sécurisée afin de garantir la confidentialité de l'identité de l'auteur du signalement et de tout tiers mentionné dans le signalement, et dont l'accès est reservé aux seules personnes habilitées (ci-après, les "Personnes de Confiance d'Intégrité ou "PCI" ou "Gestionnaire de Signalement"). La composition du groupe PCI est renseignée infra.

Tout autre membre du personnel non autorisé ne peut avoir accès au contenu des signalements.

Il est à noter que **les signalements anonymes sont autorisés.**

Vous pouvez ainsi effectuer un signalement (y compris de manière anonyme) à travers l'un ou plusieurs des moyens internes suivants :

- L'adresse mail : lanceurdalerte@paradigm.brussels
- Au téléphone : 02.801.00.10
- Par correspondance : Enveloppe scellée portant la mention STRICTEMENT CONFIDENTIEL et adressée au Groupe PCI. Un box est mis à disposition à cet effet.
- A l'occasion d'un rendez-vous (demande de rendez-vous à introduire par mail à l'adresse mentionnée ci-dessus ou au téléphone au numéro indiqué ci-dessus) avec une des Personnes du groupe PCI.

Le groupe PCI de PARADIGM est composé des personnes suivantes :

- Chief Information Security Officer : Alain Houbaille
- Service Head – Administration & Reward : Frédéric Lo Dico
- Service Head - Juridique : Nassiba Mechedal

Le lanceur d'alerte communique les faits, informations et documents utiles, sous quelque forme ou quelque support que ce soit, ainsi que les éléments permettant de prendre contact avec lui au travers du formulaire disponible en annexe ou sur l'intranet.

Afin que le Gestionnaire de Signalement soit en mesure d'examiner correctement votre signalement, il convient de fournir dans la mesure du possible les informations suivantes:

- Votre relation avec Paradigm(p.ex. travailleur, fournisseur...) ;
- Si vous souhaitez effectuer un signalement nominatif : vos nom et prénom (sauf signalement anonyme) ;
- Une description détaillée de l'incident ou de l'infraction répondant aux questions suivantes :
  - Que s'est-il passé ?
  - Quand l'incident s'est-il produit (date et heure ou période) ?
  - Où l'incident s'est-il produit ?
  - Quel a été votre rôle ou votre implication dans l'incident (p. ex. témoin, victime, auteur) ?
- Éventuellement des informations sur les personnes impliquées :
  - Nom et coordonnées des personnes impliquées dans l'incident ;
  - Nom et coordonnées de personnes qui ont été témoins de l'incident ou qui pourraient posséder de plus amples informations à ce sujet ;
- Éventuellement des informations sur des infractions ou incidents antérieurs similaires concernant la ou les personnes mentionnées dans le signalement ;

Le signalement peut être accompagné d'éventuelles pièces justificatives ou documents utiles si le canal interne utilisé pour le singalement le permet, étant rappelé qu'il est possible d'utiliser plusieurs moyens internes de signalement pour une même alerte en renseignant le numéro de dossier obtenu lors du premier signalement.

IV. Suivi des signalements

Réception et prise en charge des signalements :

Tout signalement à travers les moyens énumérés ci-dessus est reçu et pris en charge par la Personne de Confiance d'Intégrité qui en assurera un traitement confidentiel.

Accusé de reception et retour d'information :

Après réception du signalement, la Personne de Confiance d'Intégrité fournira à l'auteur du signalement :

- Un accusé de réception du signalement, accompagné d'une brève description des étapes suivantes et d'une mention selon laquelle le signalement peut ou non être 'protégé' au sens des textes applicables en la matière[2], et le cas échéant de l'identité du Gestionaire de Signalement, dans les 7 jours de la réception du signalement écrit ou de la preuve du signalement oral jointe au signalement.

[2] *Pour rappel : La directive de l'Union Européenne 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union européenne et ses textes de transposition en droit belge, à savoir la loi de transposition du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique tant du secteur privé que du secteur public, et les décret et ordonnance conjoints de la COCOM-COCOF du 27 avril 2023 modifiant les décret et ordonnance conjoints des 26 avril et 16 mai 2019 relatifs au médiateur bruxellois, accompagnés de l'Arrêté du Gouvernement de la Région de Bruxelles-Capitale du 7 décembre 2023 portant exécution de l'article 15, §2 des décret et ordonnance conjoints de 2019 précité.*

- Un retour d'informations sur les suites données au signalement, dans un délai de 3 mois à compter de l'accusé de reception : Les suites données au signalement peuvent être :
    - Irrecevable (si les éléments en possession du Gestionnaire de signalement sont insuffisants à établir que l'atteinte suspectée à l'intégrité a été commise);
    - Ouverture d'une enquête interne (si les éléments en possession du Gestionnaire de signalement permettent d'établir que l'atteinte suspectée à l'intégrité est susceptible d'avoir été commise);
    - Renvoi vers le service competent auprès du Médiateur bruxellois en cas de moyens d'investigation du service interne competent insuffisant ou en cas de risques de conflits d'intérêts ou d'immixtion.

Information du résultat de l'enquête : Si une enquête est ouverte, à l'issue de l'enquête, la Personne de Confiance d'Intégrité informera l'auteur du signalement du résultat de l'enquête et les personnes qui ont été contactées dans le cadre de l'enquête seront informées de la fin de l'enquête. L'enquête est clôturée au plus tard dans les 3 mois suivant la decision d'ouverture de l'enquête (sauf délai supplémentaire de 9 mois maximum pour des motifs dûment justifiés).

Vous pouvez à tout moment, d'initiative ou sur demande du Gestionnaire de Signalement, par écrit ou oralement, fournir des explications supplémentaires quant à l'atteinte suspectée à l'intégrité signalée. Toute personne jugée appropriée pourra être entendue, avec droit d'assistance par un avocat ou par un representant synodical.

Il est rappelé que le Gestionnaire de signalement est tenu à un suivi diligent, en ce compris, pour les singalements anonymes. Il est également précisé que le législateur a autorisé le Gestionnaire de Signalement à communiquer des informations confidentielles en vue de garantir un retour d'informations tel que précité.

Dans le cas où le signalement effectué n'est pas couvert par la présente politique, vous serez orienté(e) vers les instances compétentes. Vous en serez préalablement avisé(e), et aurez la possibilité de vous y opposer dans les plus brefs délais moyennant une raison valable.

Archivage du signalement :

Le Gestionnaire de Signalement consigne les signalements dans un registre dédié et tenu en interne de manière confidentielle et dont l'accès sécurisé est limité aux personnes habilitées, afin de garantir le respect des exigences de confidentialité. Les signalements seront conservés pendant 10 ans à compter de la cloture de la procéure de signalement, selon les formes légales.

V. Conditions de recevabilité du signalement

Pour bénéficier de la protection des lanceurs d'alerte, vous devez remplir les conditions suivantes :

- ✓ Avoir des motifs raisonnables de croire en la véracité des informations signalées; et
- ✓ Avoir suivi la procédure de signalement prévue par la règlementation relative aux lanceurs d'alerte ci-dessus rappelée.

Nous attirons votre attention sur le fait que la personne qui est sciemment à l'origine de révélations ou de signalements malveillants ou incorrects encourt des sanctions disciplinaires et/ou pénales.

VI. Etendue de la protection accordée aux lanceurs d'alerte

Protection contre toute forme de représailles :

Le lanceur d'alerte bénéficie d'une protection contre **toute forme de représailles, y compris menaces et tentatives de représailles**, incluant notamment les formes suivantes : licenciement, rétrogradation ou refus de promotion, intimidation et mise sur liste noire, suspension, transfert de fonctions, changement de lieu de travail, réduction de salaire, la modification des horaires de travail, suspension de la formation, évaluation de performance ou attestation de travail négative, mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière, mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière, coercition, intimidation, harcèlement ou ostracisme, discrimination, non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire, résiliation anticipée ou annulation d'un contrat pour des biens ou des services, annulation d'une licence ou d'un permis...

En cas de signalement anonyme, vous êtes également protégé.e si votre identité est révélée ultérieurement et que vous subissez des représailles.

Lorsque vous avez effectué un signalement et que vous bénéficiez de la protection dont il est question dans ce paragraphe, la charge de la prevue qu'il ne s'agit par de représailles et qu'une telle mesure est dûment justifiée et est étrangère au fait que la personne concernée ait effectué un signalement, incombe à l'employeur.

Protection de l'identité de l'auteur du signalement :

Le Gestionnaire de Signalement répond à l'**interdiction de divulgation, directe ou indirecte, de toute information permettant d'identifier l'identité de l'auteur du signalement**. A ce titre, le Gestionnaire de Signalement assure la confidentialité de votre identité, ainsi que de toute autre information à partir de laquelle votre identité peut être directement ou indirectement déduite.

Sauf votre consentement exprès, le Gestionnaire de Signalement ne doit révéler votre identité à d'autres personnes autre que les membres du personnel autorisés compétents pour recevoir des signalements ou en assurer le suivi.

Il est précisé que votre identité peut être divulguée lorsqu'il s'agit d'une obligation nécessaire et proportionnée dans le cadre d'une enquête, de poursuites ou d'une procédure judiciaire, notamment en vue de sauvegarder les droits de la défense de la personne concernée par la divulgation. Vous serez informé.e préalablement par écrit de la divulgation et des motifs qui justifient cette divulgation, sauf si une telle information risque de compromettre une enquête, des poursuites ou une procédure judiciaire en cours.

Protection des données à caractère personnel :

Le Gestionnaire de Signalement assure la **protection de vos données à caractère personnel.**

Il est rappelé que le responsable du traitement peut limiter le droit d'accès aux données de toute personne concernée par le signalement, visée par le signalement et/ou concernée par le suivi du signalement pour assurer 1) l'effectivité de l'enquête, des recherches ou de la procédure judiciaire et 2) la protection des droits et libertés de la personne ayant effectué le signalement.

Tout refus/limitation d'accès ainsi que les motifs du refus/limitation vous seront communiquées dans les meilleurs délais, sauf si une telle communication risque de compromettre 1) l'effectivité de l'enquête, des recherches ou de la procédure judiciaire ; 2) la protection des droits et libertés de la personne ayant effectué le signalement.

Si vous estimez que l'organisme concerné par le signalement n'assure pas une protection suffisante de vos données à caractère personnel, vous pouvez saisir l**e-la Délégué.e à la protection des données** (Rue de la Presse 35, 1000 Bruxelles - dpo@apd-gba.be).

Il vous est également possible de faire une reclamation en vous adressant à **l'Autorité de Protection des Données** (Rue de la Presse 35, 1000 Bruxelles - Tél. + 32 2 274 48 00 – Fax. + 32 2 274 48 35 – contact@apd-gba.be).

Demande d'être placé sous la protection du Médiateur :

Enfin, en tant que lanceur d'alerte vous pouvez faire la demande au Gestionnaire de Signalement d'être placé sous la protection du Médiateur bruxellois si vous craignez que votre protection ne soit pas assurée par l'organisme concerné par le signalement.

VII. Mesures de soutien

En tant que lanceur d'alerte, vous bénéficiez :

- d'informations et de conseils indépendants, ainsi que
- d'une assistance juridique conformément aux règles européennes dans le cadre des procédures pénales et civiles transfrontières.

En Belgique, les informations et le soutien se font par l'intermédiaire des instances suivantes (dont les coordonnées sont au point VIII des présentes) :

- La Médiatrice bruxelloise : elle examine les signalements de tout membre du personnel d'une administration bruxelloise qui a connaissance d'une atteinte à l'intégrité portant préjudice à l'intérêt public.
- Le Médiateur fédéral : il agit en tant que coordinateur fédéral des signalements externes.
- L'Institut Fédéral pour la Protection et la Promotion des Droits Humains (IFDH) : il fournira aux lanceurs d'alerte un soutien professionnel, juridique et psychologique.

VIII. Canaux externes de signalement

Il est rappelé qu'il existe des canaux externes de signalement.

A ce titre, vous pouvez notamment vous addresser aux autorités suivantes :

- **La Médiatrice Bruxelloise** :

  Ombuds Bruxelles
  Place de la Vieille Halle aux Blés 1
  1000 Bruxelles
  Portail sécurisé
  Téléphone : +32 2 549 67 00
  Mail : integrite@ombuds.brussels
  Rendez-vous (par mail ou par téléphone)

- **Les Médiateurs Fédéraux** - qui transmettront les signalements à l'autorité compétente

  Médiateurs fédéraux
  Rue de Louvain, 48, boîte 6
  1000 Bruxelles
  Téléphone : 0800 99 961 ou +32 2 289 27 27
  E-mail

- **L'Institut fédéral pour la protection et la promotion des droits humains (IFDH)** - il le point central d'information en ce qui concerne la protection des auteurs de signalement **:**

  IFDH
  Rue de Louvain, 48
  1000 Bruxelles
  E-mail