proximus

Group Compliance

Procédure de lanceur d'alerte

Dernière révision	03/10/2023
Responsable	Maurizio Carlone – Manager Group Compliance
Contact	group.compliance@proximus.com

Table des matières

Table des matières.....1

1. Qu'est-ce qu'un lanceur d'alerte ? 2

2. Cadre législatif et champ d'application 2

3. Qui peut signaler un problème ? 3

4. Quels types d'atteintes à l'intégrité peuvent être soulevées ? 3

5. Comment faire part d'un problème ? 4

5.1 Canaux de signalement internes 4

5.2 Canal de signalement externe 5

5.3 Institut fédéral pour la protection et la promotion des droits humains (IFDH) 5

5.4 Rester anonyme 5

5.5 Le suivi 6

5.6 Devoir de confidentialité 6

6. Protection du lanceur d'alerte 7

7. Processus de surveillance du contrôle de conformité 7

8. Traitement des données personnelles 7

1. Qu'est-ce qu'un lanceur d'alerte ?

Les lanceurs d'alerte sont des **personnes**, qui travaillent pour une organisation ou sont en contact avec une organisation dans le cadre de leurs activités professionnelles, **qui font un signalement lorsqu'elles sont confrontées à des actes répréhensibles dans le cadre de leur travail**.

Les rapports des lanceurs d'alerte sont importants car ils peuvent conduire à la détection, à l'investigation et au suivi efficaces d'actes répréhensibles et/ou de violations du code de conduite, des politiques et procédures internes, des lois et des règlements qui, autrement, resteraient cachés. Les lanceurs d'alerte contribuent ainsi à construire et à assurer l'avenir du Groupe Proximus, en atténuant le risque d'atteinte à la réputation et en limitant les pertes financières.

2. Cadre législatif et champ d'application

Les législations européennes et belges ont récemment renforcé le cadre juridique des dispositifs d'alerte et de protection des lanceurs d'alerte. Afin de s'y conformer, le Bureau de Conformité (« Compliance Office ») du Groupe Proximus a adapté à ces lois le **dispositif de signalement** déjà en place de manière harmonisée pour tout le Groupe Proximus. Ce dispositif permet aux employés et aux parties externes de **signaler de manière confidentielle, et anonyme pour ceux qui le désirent, toute violation non seulement du code de conduite, des politiques et procédures internes, des lois et règlements, mais aussi toute atteinte à l'intégrité** (voir point 4).

Entité	Proximus SA	Filiales belges de Proximus SA (>50% et de plus de 50 FTE)	Filiales étrangères de Proximus SA (>50%)
Cadre législatif	Loi du 8 décembre 2022 sur la protection des lanceurs d'alerte dans le **secteur public**[1]	Loi du 28 novembre 2022 réglant la protection des lanceurs d'alerte dans le **secteur privé**[2]	**Loi locale** du pays d'implantation
Canaux de signalement « internes »	Le Compliance manager de l'entité via : - Courriel - Téléphone - Courrier postal	Le Compliance manager de l'entité via : - Courriel - Téléphone - Courrier postal	Le Compliance manager de l'entité via : - Courriel - Téléphone - Courrier postal
Canal de signalement « externe »	Médiateur Fédéral	Médiateur Fédéral	Cfr loi locale
Investigation des signalements[3]	Le Compliance manager de l'entité	Le Compliance manager de l'entité	Cfr loi locale
Rôle du Bureau de Conformité du Groupe (« Group Compliance Office »)	Conseil, expertise et reporting	Conseil, expertise et reporting	Conseil, expertise et reporting

[1] Loi secteur public
[2] Loi secteur privé
[3] En cas d'externalisation à un tiers de la gestion du canal de signalement, le Compliance manager de l'entité du Groupe Proximus concernée reste responsable.

3. Qui peut signaler un problème ?

Cette procédure est applicable à **toute personne ayant acquis des informations sur des manquements dans un contexte professionnel** au sein du Groupe Proximus. Ces personnes peuvent avoir notamment le statut de travailleur, d'ancien ou de futur travailleur, d'entrepreneur, de fournisseur, d'actionnaire ou appartenir à l'organe d'administration, de gestion ou de surveillance d'une entreprise, y compris les membres non exécutifs, ainsi que les bénévoles et les stagiaires rémunérés ou non.

4. Quels types d'atteintes à l'intégrité peuvent être soulevées ?

L'alerte doit concerner directement les activités de Proximus ou une de ses filiales et ne peut avoir trait à des litiges personnels qui n'ont rien à voir avec les actes repris dans cette politique ou encore à des accusations que vous savez fausses.

Pour bénéficier des protections visées au point n°6, le signalement **doit porter sur l'un des éléments suivants** :

Proximus SA	Filiales belges de Proximus SA (>50% et de plus de 50 FTE)
(i) L'exécution ou l'omission d'un acte qui constitue une menace pour l'intérêt général ou une atteinte à celui-ci, et qui : - constitue une violation aux dispositions européennes directement applicables, aux normes belges, et aux règles et procédures internes à Proximus SA ; - implique un risque pour la vie, la santé ou la sécurité des personnes ou de l'environnement ; et/ou - témoigne d'un manquement grave aux obligations professionnelles ou à la bonne gestion d'un organisme du secteur public fédéral. (ii) Le fait de donner l'ordre ou de conseiller sciemment de commettre une atteinte à l'intégrité telle que décrite ci avant.	(i) Les violations des dispositions européennes directement applicables ou de normes belges qui concernent les domaines suivants : - marchés publics ; - services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme; - sécurité et conformité des produits; - sécurité des transports; - protection de l'environnement; - radioprotection et sûreté nucléaire; - sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux; - santé publique; - protection des consommateurs; - protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information; - lutte contre la fraude fiscale; - lutte contre la fraude sociale. (ii) les violations portant atteinte aux intérêts financiers de l'Union européenne. (iii) les violations relatives au marché intérieur de l'Union européenne, dans lequel est garantie la libre circulation des marchandises, des personnes, des services et des capitaux, y compris les violations des règles de l'Union en matière de concurrence et d'aides d'Etat.

N'utilisez pas les canaux de signalement décrits dans cette politique pour signaler une menace immédiate à la vie, à la santé et à la sécurité ou aux biens ou pour les griefs que vous pourriez avoir concernant vos conditions de travail.

En particulier, notez que **les plaintes relatives aux éléments suivants ne doivent pas être effectuées par le biais de la procédure de signalement (interne ou externe), mais selon d'autres procédures plus particulières** en vertu desquelles vous bénéficierez également d'une protection spécifique :

- **La violence, le harcèlement moral et sexuel au travail.** Ce type de plaintes doit être adressé à la personne de confiance de votre organisation ou au conseiller en prévention (loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail) ;
- **La discrimination.** Les plaintes pour discrimination doivent être adressées, selon le cas, à Unia (Centre interfédéral pour l'égalité des chances) ou à l'Institut pour l'égalité des femmes et des hommes (lois anti-discrimination)[4].

5. Comment faire part d'un problème ?

Chaque entité du Groupe Proximus dispose d'un canal de signalement interne en plus du canal de signalement externe qui est prévu par la loi.

La loi garantit le libre choix entre ces deux canaux. Nous recommandons, mais sans aucune obligation, de commencer par le canal interne, avant de passer par le canal externe. En utilisant la voie interne, le problème peut être traité efficacement en interne par le Compliance manager de l'entité concernée. Cela permet de prendre le plus rapidement possible des mesures efficaces de redressement.

5.1 Canaux de signalement internes

Si vous avez connaissance d'une atteinte à l'intégrité, telle qu'énoncée ci-dessus (voir point 4) vous pouvez signaler le problème ou l'infraction directement en utilisant l'un des **canaux d'alerte suivants afin que votre signalement soit traité de manière confidentielle et votre protection légale assurée** :

Par téléphone (du lundi au vendredi de 09:00 à 17:00) : +32 (0) 800 45 002

Par courriel : whistleblower@proximus.com

Par courrier à l'une des personnes suivantes (veuillez bien indiquer « confidentiel » sur l'enveloppe) :

- **Compliance manager du Groupe Proximus** : Proximus – Maurizio Carlone, Group Compliance, 27 Boulevard du roi Albert II, B 1030 Bruxelles
- **Président du Comité d'Audit et de Conformité** : Proximus – Catherine Vandenborre, Présidente du Comité d'audit et de conformité, 27 Boulevard du roi Albert II, B 1030 Bruxelles.

En prenant **rendez-vous** avec le Compliance manager ou le Président du Comité d'Audit et de Conformité via le canal téléphonique ou par courriel.

[4] la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination ; la loi du 10 mai 2007 tendant à lutter contre la discrimination entre les femmes et les hommes ; la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie.

5.2 Canal de signalement externe

Un canal de signalement externe a été désigné par l'État belge. Il s'agit du **Centre Intégrité du Médiateur Fédéral** que vous pouvez contacter comme suit :

En ligne : via le Centre Intégrité | Federaalombudsman.be

Par téléphone : du lundi au vendredi de 9h00 à 12h30 et de 13h30 à 17h00 :

- Depuis la Belgique via le numéro gratuit 0800 99 961
- Depuis l'étranger via le +32 2 289 27 27

Par courriel : contact@mediateurfederal.be

5.3 Institut fédéral pour la protection et la promotion des droits humains (IFDH)

L'IFDH est le point central d'information en matière de protection des auteurs de signalement. Il est notamment chargé d'appliquer ou de veiller à l'application de mesures de soutien auxquelles ont droit les auteurs de signalement. Il s'agit du bénéfice :

- d'informations et de conseils complets et indépendants, qui sont facilement accessibles au public et gratuits, sur les procédures et les recours disponibles, sur la protection contre les représailles, ainsi que sur les droits de la personne concernée, y compris ses droits au niveau de la protection des données à caractère personnel ;
- des conseils techniques devant toute autorité qui est associée à la protection de l'auteur de signalement ;
- d'une assistance juridique ainsi que des conseils juridiques ou toute autre assistance juridique, tels que l'aide juridique de deuxième ligne et l'assistance judiciaire, dans le cadre des procédures pénales et civiles, conformément aux articles 495, alinéa 3, 508/7 à 508/25, 664 à 699ter, et 1723/1 à 1737 du Code judiciaire, à l'article 47bis du Code d'instruction criminelle, aux articles 2bis, 16 et 24bis/1 de la loi du 20 juillet 1990 relative à la détention préventive, et aux articles 10/1, 10/3 et 34/1 de la loi du 19 décembre 2003 relative au mandat d'arrêt européen ;
- des mesures de soutien, y compris de nature technique, psychologique, médiatique et sociale ;
- d'une assistance financière pour les auteurs de signalement dans le cadre des procédures judiciaires.

Contact de l'IFDH :

Par téléphone : 0479/88.57.23

Par courriel : kl-la@firm-ifdh.be

Par courrier : Institut Fédéral des Droits Humains (IFDH), Rue de Louvain 48, 1000 Bruxelles

https://www.federalinstitutehumanrights.be/fr/vous-avez-des-questions-contactez-nous

5.4 Rester anonyme

Vous pouvez déposer une plainte de manière anonyme. Cela signifie que même le destinataire de la plainte ne connaîtra pas votre identité. Pour ce faire vous pouvez **envoyer votre plainte par lettre**. Nous insistons pour que vous indiquiez CONFIDENTIEL sur l'enveloppe afin que votre lettre suive le processus de traitement confidentiel par nos services postaux internes.

Un rapport anonyme ne sera considéré comme valide que s'il contient suffisamment d'éléments factuels permettant d'enquêter sur les faits. Par conséquent, veuillez **inclure autant de détails que possible** dans l'intérêt de l'aboutissement d'enquête et du suivi d'une dénonciation anonyme.

Proximus est tenue d'accepter les signalements anonymes. Toutefois, nous vous recommandons de décliner votre identité lorsque vous signalez un problème. En effet, l'anonymat doit rester exceptionnel dès lors qu'il peut notamment rendre difficile la communication entre l'auteur du signalement et le destinataire dudit signalement, ce qui peut pourtant être nécessaire pour un suivi diligent. De cette manière, nous saurons, par exemple, qui nous devons protéger (vous et les facilitateurs ou tiers concernés) et à qui nous pourrons nous adresser pour obtenir des informations complémentaires afin que personne ne soit accusé à tort sur la base d'informations erronées.

5.5 Le suivi

Après avoir procédé à une dénonciation en utilisant le canal interne, vous recevrez un **accusé de réception dans les 7 jours calendrier (maximum).**

La personne responsable du suivi de votre alerte l'enregistrera dans un registre séparé. Elle entamera une enquête préliminaire pour vérifier si la préoccupation rentre bien dans le cadre prévu par la loi et semble fondée. Cette personne restera également en contact avec vous et, si nécessaire, vous demandera des informations complémentaires.

Vous serez **informé dans un délai de maximum 3 mois (après l'accusé de réception)** de la suite donnée au signalement.

L'identité du lanceur d'alertes sera toujours tenue confidentielle.

5.6 Devoir de confidentialité

Lorsque vous signalez un problème, le secret de votre identité en tant que lanceur d'alerte sera garanti conformément aux lois et règlements applicables.

Votre identité ne sera pas divulguée sans votre consentement explicite, en dehors des personnes autorisées et compétentes de la réception et du suivi des rapports. Cela s'applique également à toute autre information à partir de laquelle votre identité peut être (in)directement déduite.

Ce n'est que s'il existe une obligation nécessaire et proportionnée imposée par le droit européen ou national dans le cadre d'enquêtes menées par les autorités nationales ou de procédures judiciaires que votre identité ou une information de laquelle elle peut être déduite pourrait être divulguée, y compris en vue de sauvegarder les droits de la défense de la personne concernée.

Tenez compte qu'un rapport anonyme ne sera considéré comme valide que s'il contient suffisamment d'éléments factuels permettant d'enquêter sur les faits. Par conséquent, veuillez inclure autant de détails que possible dans l'intérêt même de l'aboutissement de l'enquête (voir point 5.4).

Dans le cadre de cette politique, Proximus et ses filiales peuvent collecter des données personnelles sur base des obligations qui lui sont imposées par la directive européenne et les lois nationales, dans le strict respect du Règlement général sur la protection des données (RGPD), et uniquement dans la mesure nécessaire pour les besoins de l'enquête et la prise de mesures correctrices. Toutes les données personnelles collectées dans le cadre de cette procédure seront traitées tel qu'expliqué à la section 8 ci-dessous.

6. Protection du lanceur d'alerte

La loi a considérablement renforcé la protection des lanceurs d'alertes contre les représailles et la sévérité des sanctions contre les auteurs de ces représailles. Aucun lanceur d'alerte qui signale un événement sur la base de motifs raisonnables ne peut faire l'objet de représailles (par exemple, être sanctionné ou faire l'objet d'une quelconque mesure discriminatoire) pour avoir notifié une alerte via les mécanismes de lanceur d'alerte. **Le Groupe Proximus interdit et sanctionne toutes formes de représailles à l'encontre de ceux qui, de bonne foi, signalent une infraction ou un soupçon d'infraction.**

Si vous signalez un problème et qu'il s'avère que vous vous êtes sincèrement trompé, vous ne serez pas sanctionné. Les mesures de protection s'étendent également aux facilitateurs et aux tiers ayant un lien professionnel ou familial avec l'auteur du signalement.

Si en raison de votre alerte, vous vous sentez menacé ou faites l'objet de représailles, nous vous invitons soit de réintroduire un signalement auprès du canal de signalement interne, soit d'introduire un signalement directement auprès du canal de signalement externe dont une des missions prévues par la loi est de vous offrir une protection contre les représailles. Vous pouvez de plus demander l'assistance de l'IFDH[5] dans vos démarches (voir point 5.3).

7. Processus de surveillance du contrôle de conformité

Un plan de contrôle spécifique développé par le Bureau de Conformité du Groupe Proximus (« Group Compliance Office ») vérifiera la bonne implémentation de cette procédure.

8. Traitement des données personnelles

Cette section décrit comment les entités du Groupe Proximus traitent vos données personnelles en leur qualité de responsable du traitement dans le cadre de la présente procédure de lanceur d'alertes. Ces informations s'adressent à tout lanceur d'alerte et à toute personne qui fait l'objet d'un signalement.

- **Catégories de données personnelles :** Nous pouvons collecter et traiter les catégories de données personnelles suivantes lorsqu'un signalement est effectué via les canaux de signalement décrits dans cette politique :
    - l'identité, les fonctions et les coordonnées du lanceur d'alerte (dans le respect des règles de confidentialité mentionnées à la section 5.4), des personnes mentionnées dans le signalement et des personnes impliquées dans la réception et le suivi du signalement ; et
    - les événements signalés, les informations recueillies au cours de l'enquête, et toute mesure prise à la suite de l'enquête, dans la mesure où ces informations sont liées à des données personnelles.
- **Finalités :** Nous traitons les données personnelles susmentionnées aux fins de la gestion des signalements et de la détection, l'investigation et le suivi d'actes répréhensibles ou de violations du code de conduite, des politiques et procédures internes, des lois et des règlements.

[5] FIRM-IFDH (federalinstitutehumanrights.be)

- **Bases juridiques** : Comme expliqué au point 2 de cette procédure, nous avons l'obligation légale de mettre des canaux de signalement à disposition pour certains types d'infractions. Lorsque le signalement relève de cette **obligation légale**, c'est sur cette base juridique que nous traiterons ces données. Pour tout autre signalement, nous nous appuyons sur nos **intérêts légitimes** qui consistent à nous assurer que la conduite de nos collaborateurs soit conforme à ce qui est exigé par la loi, par les normes du secteur et par les politiques et normes internes de Proximus.
- **Destinataires des données** : Seules les personnes autorisées et compétentes pour la réception et le suivi des rapports au sein du Groupe Proximus ont accès aux données personnelles susmentionnées. Ce n'est que si nous y sommes légalement obligés que ces données peuvent être communiquées aux autorités nationales ou de procédures judiciaires.
- **Conservation des données** : Les données personnelles obtenues dans le cadre d'un signalement sont conservées aussi longtemps que nécessaire pour traiter le signalement, y compris ses éventuelles conséquences, comme les actions en justice. Les données personnelles qui ne sont manifestement pas pertinentes pour le traitement d'un signalement spécifique ne sont pas collectées ou, si elles le sont accidentellement, sont effacées sans retard. Le nom, la fonction et les coordonnées de l'auteur de signalement ainsi que de toute personne à qui les mesures de protection et de soutien s'étendent, ainsi que de la personne concernée, en ce compris, le cas échéant son numéro d'entreprise, sont sauvegardés jusqu'à ce que la violation signalée soit prescrite. En ce qui concerne Proximus SA, celle-ci ne conservera les données à caractère personnel dans le cadre des signalements qu'elle reçoit que pendant la durée de l'enquête sauf si des procédures judiciaires ou des mesures disciplinaires sont engagées contre la personne concernée, contre l'auteur de signalement ou contre toute autre personne impliquée dans le dossier. Dans ces cas, Proximus conservera les données à caractère personnel jusqu'à ce que les procédures en question soient clôturées et les délais pour intenter un recours, écoulés.
- **Vos droits** :
    - Droit d'accès : Vous avez le droit de nous interroger sur les données à caractère personnel dont nous disposons à votre sujet. Nous pouvons vous en fournir une copie gratuitement, mais ce n'est pas possible pour tous les documents. Nous entendons en effet aussi respecter les droits et libertés d'autrui.
    - Droit de rectification : Vous pensez que vos données ne sont pas exactes ou actuelles ? Vous avez le droit de nous demander de les corriger.
    - Droit d'opposition : Dans les conditions prévues par la loi (notamment à l'article 21 du RGPD), vous avez le droit de nous demander d'arrêter de traiter vos données à caractère personnel.
    - Droit à la limitation du traitement : Vous pouvez nous demander de limiter le traitement de vos données à caractère personnel, par exemple lorsque nous vérifions l'exactitude de vos données à caractère personnel.
    - Droit à l'oubli ou à la suppression : Dans les conditions prévues par la loi (notamment à l'article 17 du RGPD), vous avez le droit de nous demander de supprimer vos données à caractère personnel.

  Vous pouvez exercer vos droits en contactant le délégué à la protection des données de Proximus : privacy@proximus.com. Vous avez aussi le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente. En Belgique, cette autorité est l'Autorité de protection des données :
    - Rue de la Presse 35, 1000 Bruxelles
    - +32 (0)2 274 48 00
    - contact@apd-gba.be

  Veuillez noter que, dans la mesure où l'exercice de vos droits repris aux articles 14 (droit d'information lorsque les données personnelles ne sont pas collectées auprès de la personne concernée), 15 (droit d'accès) et 16 (droit de rectification) du RGPD risque d'entraver, d'empêcher, d'obstruer ou de retarder le suivi du signalement ou les demandes de protection ou d'identification des auteurs du signalement, il est possible pour Proximus SA de déroger à ces droits. Malgré ces restrictions, vous conservez la possibilité d'intenter une action en justice conformément à l'article 79 du RGPD et de déposer une plainte auprès de l'autorité de contrôle conformément à l'article 77 du RGPD.