BIOSerenity

Charte Lanceur d’alerte

2025

Table des matières

1. INTRODUCTION

1.1 Les trois canaux de signalement prévus par la loi

Le lanceur d'alerte dispose de trois canaux distincts pour effectuer son signalement tout en bénéficiant des protections accordées par la loi à ce statut :

A. Signalement interne : le lanceur d'alerte choisit de déposer l'alerte en interne via la Ligne Ethique ou directement auprès de toute autre personne habilitée ; c'est l'objet de la présente politique.

B. Signalement externe : le lanceur d'alerte peut adresser son alerte à toute autorité compétente telle que listée en annexe au décret n°2022-1284 du 3 octobre 2022, ou encore au Défenseur des droits, à l'autorité judiciaire ou à toute institution, organe ou organisme de l'Union européenne compétent. Ce signalement externe peut intervenir soit après un signalement interne, soit directement lorsque le lanceur d'alerte estime qu'il n'est pas possible de remédier efficacement à la situation par un signalement interne ou qu'il s'expose à un risque de représailles.

C. Divulgation publique : le lanceur d'alerte peut rendre l'alerte publique dans certaines conditions précises :

- Soit après signalement externe et dans la mesure où celui-ci n'a été suivi d'aucune mesure appropriée dans les délais fixés ;
- Soit en cas de danger grave et imminent ;
- Soit lorsque la saisine de l'autorité compétente ferait courir au lanceur d'alerte un risque de représailles ou ne permettrait pas de remédier efficacement à la situation, en raison des circonstances particulières de l'affaire.

Le dispositif d'alerte mis en place par BIOSerenity porte exclusivement sur le signalement interne visé au (A) ci-dessus.

1.2 Le dispositif interne au Groupe BIOSerenity – champ d'application

Le Groupe BIOSerenity promeut la conformité aux lois et réglementations applicables, en particulier celles rappelées dans sa Charte Ethique.

Dans une démarche d'amélioration continue et afin de prévenir ou limiter les risques auxquels l'une des entités du Groupe BIOSerenity et/ou l'un de ses employés pourrait être confronté(e), les collaborateurs, contractants, partenaires ou parties prenantes qui le souhaitent peuvent utiliser le dispositif d'alerte professionnelle mis en place par BIOSerenity afin de signaler tout manquement à ces règles, qu'il soit potentiel ou avéré.

La présente politique s'adresse donc à l'ensemble de ces personnes et couvre tout signalement effectué par le canal interne, que ce soit à travers l'adresse mail dédiée ou auprès des personnes habilitées en interne. L'adresse mail dédiée (« MyEthics ») permettant de déposer une alerte est la suivante : ethics@bioserenity.com

1.3 Les textes

La présente politique est adoptée par BIOSerenity en application de la loi n°2016-1691 du 9 décembre 2016 dite « loi Sapin 2 » (articles 6 à 17) telle que modifiée par la loi n°2022-401 du 21 mars 2022 et complétée par le décret n°2022-1284 du 3 octobre 2022.

1.4 Les sanctions

Afin d'encourager le dépôt d'alertes professionnelles et de protéger les lanceurs d'alertes, la loi réprime un certain nombre de manquements aux exigences posées :

- Toute personne qui fait obstacle, de quelle que façon que ce soit, à la transmission d'une alerte est punie d'un an d'emprisonnement et 15 000 euros d'amende pour les personnes physiques (art. 13 I. de la loi Sapin 2) ;
- Toute violation de la confidentialité de l'alerte, du lanceur d'alerte, de la personne visée par l'alerte ou de personnes mentionnées dans l'alerte est punie de 2 ans d'emprisonnement et 30.000 euros d'amende (article 9, II de la loi Sapin 2) ;
- Toute discrimination fondée sur la « qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte » est punie de trois ans d'emprisonnement et de 45.000 euros d'amende (articles 225-1 et 225-2 du Code pénal) ;
- En outre, les procédures dilatoires ou abusives intentées contre un lanceur d'alerte peuvent être sanctionnées par une amende civile de 60.000 euros, sans préjudice de l'octroi de possibles dommages et intérêts ainsi que le prononcé d'une peine de diffusion de la décision (article 13 II de la loi Sapin 2).

Les amendes prévues pour les personnes physiques sont multipliées par cinq pour les personnes morales.

1.5 Communication de la politique

Conformément au décret 2022-1284 du 3 octobre 2022, « La procédure est diffusée par l'entité concernée par tout moyen assurant une publicité suffisante, notamment par voie de notification, affichage ou publication, le cas échéant sur son site internet ou par voie électronique, dans des conditions permettant de la rendre accessible de manière permanente aux personnes mentionnées » au chapitre 4 ci-dessous.

Les recommandations de l'Agence française anticorruption rappellent également que les différentes étapes de la mise en œuvre du dispositif d'alerte devraient comporter la *« diffusion de la procédure d'alerte interne à l'ensemble des personnels par tous moyens (courrier de la direction, affichage, site intranet, remise en main propre, etc.) permettant de s'assurer que chaque personne concernée en a connaissance et y a accès. Dans le cas d'un dispositif d'alerte commun à l'alerte anticorruption et à d'autres dispositifs légaux, la procédure doit être également diffusée aux collaborateurs occasionnels. L'entreprise peut décider d'ouvrir son dispositif d'alerte aux tiers. L'entreprise peut choisir de mettre à profit ses outils de communication externes pour mentionner l'existence de son dispositif d'alerte (par exemple son site internet, les documents remis à ses tiers, etc.)* ».

Pour les collaborateurs de BIOSerenity, la procédure est notamment disponible sur la plateforme RH de la Société.

Pour les partenaires et parties prenantes de BIOSerenity, le site internet de BIOSerenity comporte un lien vers la procédure d'alerte :

https://www.BIOSerenity.com/ethique

La présente politique a été validée en Comité Exécutif au niveau de BIOSerenity et soumise à la consultation des Comités Sociaux et Economiques des sociétés du Groupe BIOSerenity.

L'utilisation du dispositif d'alerte et le traitement de ces signalements sont encadrés par les règles telles que définies ci-après.

2. FICHE PRATIQUE SUR LE DISPOSITIF D'ALERTE

Si vous êtes confronté ou assistez à :

- Un manquement aux règles de la Charte éthique de BIOSerenity ;
- Un crime ou un délit ;
- Une menace ou un préjudice grave pour l'intérêt général ;
- Une violation ou une tentative de dissimulation d'une violation du droit international ou de l'Union européenne, de la loi ou du règlement ;
- Une atteinte envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes, ainsi qu'à l'environnement.

Vous avez le choix entre :

Signalement interne auprès d'un membre de BIOSerenity : - Supérieur Hiérarchique - Conseil d'alerte	Utiliser la ligne MyEthics : ethics@bioserenity.com	Informer directement les autorités judiciaires ou administratives, le Défenseur des droits, ou l'institution/organe de l'Union Européenne compétent

L'alerte doit :

- Être émise de bonne foi et sans contrepartie financière directe par une personne physique ;
- Être fondée sur des informations dont vous avez eu personnellement connaissance si elles ont été obtenues en dehors d'un cadre professionnel ;
- Décrire les faits de manière objective et précise, en fournissant tous les éléments concrets dont vous disposez au soutien de votre alerte.

Délai de réponse :

- L'auteur de l'alerte reçoit un accusé de réception sous **sept jours** ;
- Après analyse de sa recevabilité, l'alerte fait l'objet d'un traitement dans les trois mois.

3. FAITS POUVANT DONNER LIEU A UNE ALERTE

Le dispositif d'alerte peut être utilisé pour signaler des faits susceptibles de caractériser :

- Un manquement aux règles de la Charte éthique de BIOSerenity ;
- Un crime ou un délit ;
- Une violation (ou une tentative de dissimulation d'une violation) d'un engagement international, d'un acte unilatéral d'une organisation internationale, du droit de l'Union européenne, de la loi ou du règlement ;
- Les atteintes envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement ;
- Une menace ou un préjudice pour l'intérêt général.

Dans tous les domaines, notamment :

- Financier, comptable, bancaire ;
- Lutte contre la corruption ;
- Pratiques anticoncurrentielles ;
- Santé, hygiène et sécurité au travail ;
- Lutte contre les discriminations et le harcèlement au travail ;
- Protection de l'environnement ;
- Droits de l'homme et libertés fondamentales ;

Et à l'exception des éléments couverts par :

- Le secret médical ;
- Le secret des délibérations judiciaires ;
- Le secret de l'enquête ou de l'instruction judiciaires ;
- Le secret des relations entre un avocat et son client.

Les informations peuvent porter sur des faits susceptibles de se produire ou s'étant déjà produits. En cas de doute, il est préférable d'utiliser le dispositif d'alerte plutôt que de prendre le risque qu'un fait grave ou sous-estimé ne soit pas révélé.

4. PERSONNES POUVANT LANCER UNE ALERTE

Le dispositif d'alerte peut être utilisé par :

A. Les membres du personnel des sociétés du Groupe BIOSerenity ;
B. Les personnes dont la relation de travail avec le Groupe BIOSerenity s'est terminée, lorsque les informations à l'origine de l'alerte ont été obtenues dans le cadre de cette relation ;
C. Les personnes qui se sont portées candidates à un emploi au sein de l'entité du Groupe BIOSerenity concernée, lorsque les informations à l'origine de l'alerte ont été obtenues dans le cadre de cette candidature ;
D. Les actionnaires, les associés et les titulaires de droits de vote au sein de l'assemblée générale de l'entité concernée du Groupe BIOSerenity ;
E. Les membres de l'organe d'administration, de direction ou de surveillance de l'entité concernée du Groupe BIOSerenity ;
F. Les collaborateurs extérieurs et occasionnels du Groupe BIOSerenity (consultant détaché, intérimaire, stagiaire, senior advisor, etc...) ;
G. Les cocontractants de l'entité concernée du Groupe BIOSerenity, leurs sous-traitants ou, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et de leurs sous-traitants ;
H. Ainsi que les membres du personnel des cocontractants du Groupe BIOSerenity et de leurs sous-traitants.

5. COMMENT LANCER UNE ALERTE

Toute personne répondant aux conditions décrites au paragraphe 6.2 ci-après peut déposer une alerte par le canal interne, comme suit :

A. Soit en utilisant la ligne MyEthics : ethics@bioserenity.com ;
B. Soit enfin en saisissant sa hiérarchie ou le conseil d'alerte de BIOSerenity.

Les échanges peuvent se faire sous toutes formes, par e-mail (A), par oral et, le cas échéant, lors d'une visioconférence ou d'une rencontre physique organisée au plus tard **vingt jours** ouvrés après réception de la demande (B). En tout état de cause, la confidentialité de cet échange doit être assurée par la personne qui recueille l'alerte comme par le lanceur d'alerte (voir le Chapitre 6 ci-dessous).

Il est recommandé au lanceur d'alerte de :

- Joindre des documents de nature à étayer son signalement, lorsqu'il en dispose ;
- Ne pas utiliser son matériel professionnel (ordinateur, tablette, téléphone professionnel) pour déposer son alerte ;

- Renseigner une adresse mail sur laquelle il pourra être joint dans le cadre du traitement de l'alerte. Afin de garantir la confidentialité de son identité, cette adresse mail pourra utiliser un pseudo.

Si le lanceur d'alerte choisit de rester anonyme, l'alerte ne pourra être traitée que si la gravité des faits mentionnés est établie, si les faits sont suffisamment détaillés et si le traitement de ce signalement permet de s'entourer de précautions particulières.

Si ces conditions ne sont pas réunies, le lanceur d'alerte sera invité à s'identifier pour que son alerte puisse être traitée. Le lanceur d'alerte reçoit sous **7 jours** ouvrés un accusé de réception de son alerte.

6. GARANTIES OFFERTES PAR LE DISPOSITIF D'ALERTE ETHIQUE

6.1 La confidentialité des informations recueillies dans le cadre du signalement

Le dispositif d'alerte garantit l'intégrité et la confidentialité des informations recueillies dans un signalement, conformément à l'article 9 de la loi Sapin 2.

Doivent ainsi demeurer strictement confidentielles :

A. L'identité du lanceur d'alerte[1] ;
B. L'identité de la ou des personne(s) visée(s) par l'alerte et de tout tiers mentionné dans le signalement[2] ;
C. Et plus généralement les informations recueillies dans le cadre de l'alerte, c'est-à-dire les faits faisant l'objet de l'alerte.

Par ailleurs, le lanceur d'alerte ne peut pas lui-même divulguer librement les informations objet de l'alerte.

6.2 Les conditions posées par la loi afin qu'une personne bénéficie du statut de lanceur d'alerte et des protections en découlant sont les suivantes :

A. Elle est une personne physique – elle ne peut pas être une personne morale, c'est-à-dire une entreprise, une association ou même un syndicat ;
B. Elle agit sans contrepartie financière directe ;

[1] Sauf si BIOSerenity décidait de communiquer ces faits à l'autorité judiciaire.
[2] Sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte

C. Elle agit de bonne foi – le lanceur d'alerte ne doit pas agir de façon malveillante ou par vengeance en colportant des informations qu'il sait mensongères ou erronées ;
D. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance, c'est-à-dire avoir été le témoin personnel des faits (ou la victime) – le lanceur d'alerte ne peut pas colporter une simple rumeur.

Les informations communiquées doivent rester factuelles et présenter un lien direct avec l'objet du signalement. Un lanceur d'alerte qui ne répond pas aux conditions (A) à (D), ne bénéficiera pas des protections visées au 6.3 ci-dessous et pourrait s'exposer à des sanctions disciplinaires, ainsi qu'à des poursuites judiciaires, notamment pour diffamation ou dénonciation calomnieuse.

En revanche, toute utilisation de bonne foi du dispositif d'alerte, même si les faits se révèlent, par la suite, inexacts ou ne donnent lieu à aucune suite, ne peut exposer son auteur à des sanctions ou des représailles.

6.3 La protection du lanceur d'alerte

Dès lors qu'il respecte les conditions visées au paragraphe 6.2 ci-dessus, le lanceur d'alerte bénéficie d'une large protection et notamment des garanties suivantes :

- Confidentialité des données le concernant, qui ne peuvent être divulguées sans son consentement[3] ;
- Aménagement de la charge de la preuve (i.e. il appartient à BIOSerenity de prouver que sa potentielle décision de licencier ou de sanctionner une personne à l'origine d'une alerte est motivée par des éléments objectifs étrangers à l'alerte) ;
- Protection contre les mesures de représailles (telles que suspension, licenciement, mesure disciplinaire, discrimination, traitement désavantageux…) ;
- Irresponsabilité civile (notamment si le lanceur d'alerte avait des motifs raisonnables de croire, au moment du signalement, que celui-ci était nécessaire à la sauvegarde des intérêts en cause) et pénale.

[3] Sauf si BIOSerenity décidait de communiquer ces faits à l'autorité judiciaire.

6.4 Les protections découlant du statut de lanceur d'alerte bénéficient également[4] :

- Aux facilitateurs, c'est-à-dire toute personne physique ou toute personne morale de droit privé à but non lucratif (par exemple une association ou un syndicat) qui aide un lanceur d'alerte à effectuer un signalement ;
- Aux personnes physiques en lien avec le lanceur d'alerte (par exemple des collègues ou des proches) et qui risquent de faire elles-mêmes l'objet de mesures de représailles de la part de leur employeur, de leur client ou du destinataire de leurs services.

Etant précisé que cette protection ne s'applique que si le lanceur d'alerte respecte le cadre prévu par la Loi Sapin 2 et rappelé au 6.2 ci-dessus.

6.5 Droits de la personne visée par l'alerte

Toute personne visée par une alerte (témoin, victime, auteur présumé) a droit au strict respect de sa confidentialité, notamment au regard du principe fondamental de la présomption d'innocence, du respect des droits de la défense et du respect de la vie privée.

Au titre du RGPD, elle doit être informée qu'elle est visée par une alerte, ses données personnelles faisant l'objet d'un traitement à ce titre. Pour plus de détails, voir l'annexe 1 à la présente politique.

[4] Article 2 de la loi du 21 mars 2022.

7. SUITES DONNEES A UNE ALERTE

7.1 Concernant l'alerte et l'auteur du signalement

A la suite d'un signalement interne, et dans la mesure où son auteur a renseigné une adresse mail permettant de communiquer avec lui, il reçoit sous **7 jours** un accusé de réception. Cet accusé de réception ne préjuge aucunement de la recevabilité éventuelle de l'alerte, ce point étant analysé dans un second temps.

En cas de signalement par un lanceur d'alerte auprès de son supérieur hiérarchique, le dépositaire de l'alerte est invité à en informer immédiatement le conseil d'alerte.

Le signalement fait l'objet d'un traitement par le conseil d'alerte du Groupe BIOSerenity afin d'évaluer sa recevabilité et, le cas échéant, les suites qui doivent lui être données (enquête interne, procédure judiciaire…) ainsi que les mesures de remédiation pouvant être mises en œuvre. Le conseil d'alerte peut être amené à réaliser elle-même l'enquête ou à la sous-traiter à un cabinet spécialisé.

L'auteur du signalement pourra transmettre toute information et tout document complémentaire (par écrit/oral, par e-mail ou remise en main propre) au cours de ce traitement.

L'auteur du signalement est tenu informé des suites données à son signalement dans un délai de **trois mois** à compter de l'accusé de réception. Il est également tenu informé de la clôture du dossier lié à son signalement.

7.2 Concernant la personne visée par le signalement

Toute personne visée par une alerte, que ce soit en tant que témoin, victime ou auteur présumé des faits doit en être informée dans un délai raisonnable, ne pouvant pas dépasser **un mois** à la suite de l'émission d'une alerte, sauf à ce que cette information soit susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* », tel le risque de destruction de preuves[5]. L'information doit néanmoins alors être délivrée aussitôt le risque écarté et ne doit pas contenir d'informations relatives à l'identité de l'auteur de l'alerte ni à celle de toute autre personne visée par l'alerte. L'information donnée devra mentionner l'existence du traitement, ses caractéristiques ainsi que les droits dont dispose la personne visée par l'alerte.

[5] Article 14 du Règlement Général sur la Protection des Données (« RGPD »).

Il sera également précisé à cette personne les faits qui lui sont reprochés, les services éventuellement destinataires du signalement, les modalités d'exercice de ses droits d'accès et de rectification.

L'identité de l'auteur du signalement ne pourra en aucun cas lui être communiquée.

En outre, les éléments de nature à identifier la personne mise en cause par l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte. En d'autres termes, dans le cadre du traitement de l'alerte par le conseil d'alerte du Groupe BIOSerenity, « les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions » (délibération de la CNIL du 18 juillet 2019), sauf à devoir saisir l'autorité judiciaire.

La personne mise en cause par l'alerte sera également informée de la clôture des opérations de vérification, le cas échéant, ou de la mise en œuvre d'une procédure disciplinaire ou de poursuites judiciaires. Enfin, dès lors qu'une sanction disciplinaire ou une procédure contentieuse est engagée à la suite de l'alerte à l'encontre de la personne mise en cause, cette dernière pourra obtenir communication de certains éléments de son dossier en vertu des règles de droit commun applicables, en ce compris l'identité du lanceur d'alerte et de toute autre personne visée par l'alerte, sous réserve toutefois de la prise de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées.

ANNEXE RELATIVE A LA PROTECTION DES DONNEES PERSONNELLES

1. Responsable de traitement

Le conseil d'alerte du Groupe BIOSerenity est responsable du traitement dans le cadre du dispositif d'alerte dès lors que l'alerte est effectuée par la voie hiérarchique ou via MyEthics.

2. Catégories de données à caractère personnel traitées

Dans le cadre d'un signalement, seules les catégories de données suivantes peuvent être traitées :

- Identité, fonctions et coordonnées de l'auteur du signalement
- Identité, fonctions et coordonnées des personnes faisant l'objet du signalement
- Identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement du signalement
- Faits signalés
- Eléments recueillis dans le cadre de la vérification des faits signalés
- Compte rendu des opérations de vérification
- Suites données au signalement

La prise en compte du signalement s'appuie sur des données formulées de manière objective et factuelles, par exemple, des dates, des noms et des fonctions internes des personnes impliquées, en rapport direct avec l'objet du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués.

3. Destinataires des données

Les destinataires de tout ou partie des données sont les personnes habilitées à recueillir une alerte, sous les limitations prévues au chapitre 5 ci-dessus au regard notamment de la confidentialité entourant l'identité du lanceur d'alerte.

Le conseil d'alerte du Groupe BIOSerenity se compose de :

- Un représentant du département Juridique
- Un représentant du département Ressources Humaines

- Le DPO (Délégué à la Protection des Données)

Le nom des membres du conseil d'alerte est communiqué pour information au CSE et porté à la connaissance des collaborateurs des sociétés du Groupe BIOSerenity par le même canal d'information que la présente procédure.

4. Utilisation des données

Conformément à la délibération de la CNIL (18 juillet 2019) BIOSerenity s'engage à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

5. Durée de conservation des données

Les signalements (enregistrements, transcriptions et procès-verbaux) ne peuvent être conservés que le temps strictement nécessaire et proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires.

Conformément à la délibération de la CNIL (18 juillet 2019) :

- Les données relatives à une alerte considérée par le responsable du traitement comme n'entrant pas dans le champ du dispositif, sont détruites **sans délai** du dispositif d'alertes professionnelles ou anonymisées.
- Lorsqu'aucune suite n'est donnée à une alerte entrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées dans un délai de **deux mois** à compter de la clôture des opérations de vérification.
- Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par l'organisation chargée de la gestion des alertes jusqu'au **terme de la procédure** ou de la prescription des recours à l'encontre de la décision.

A l'exception des cas où aucune suite n'est donnée à l'alerte, le responsable de traitement peut conserver les données collectées sous forme d'archives intermédiaires aux fins d'assurer la protection du lanceur de l'alerte ou de permettre la constatation des infractions continues. Cette durée de conservation doit être strictement **limitée aux finalités poursuivies**, déterminée à l'avance et portée à la connaissance des personnes concernées.

Les données peuvent être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).

En complément, conformément à la délibération de la CNIL du 12 février 2016 : « *Les données collectées et traitées dans le cadre de la gestion d'un précontentieux doivent ainsi être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante. Les données collectées et traitées dans le cadre d'un contentieux doivent quant à elles être supprimées lorsque les voies de recours ordinaires et extraordinaires ne sont plus possibles contre la décision rendue.* »

6. Droits des personnes concernées

Toute personne identifiée dans le dispositif d'alerte dispose d'un droit d'accès, de rectification, d'effacement des données et de limitation du traitement la concernant (par exemple lorsque ces données sont inexactes ou obsolètes), conformément à la règlementation applicable en France en matière de protection des données à caractère personnel.

Lorsque les personnes concernées exercent leur droit d'accès, elles ne peuvent via l'exercice de ce droit, obtenir communication d'aucune donnée relative à des tiers. En particulier, la personne visée par l'alerte qui exercerait son droit d'accès ne peut en aucun cas obtenir communication des informations concernant l'identité de l'auteur de l'alerte.

En outre, la CNIL (délibération du 18 juillet 2019) précise que le droit de rectification, prévu à l'article 16 du RGPD, doit s'apprécier au regard de la finalité du traitement. Ce droit de rectification est limité et ne peut pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectés lors de son instruction.

Son exercice, lorsqu'il est admis, ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête. Ce droit ne peut être exercé uniquement pour rectifier les données factuelles, dont l'exactitude matérielle peut être vérifiée par le responsable du traitement à l'appui d'éléments probants, et ce sans que soient effacées ou remplacées les données, même erronées, collectées initialement.

La demande doit être adressée sur la ligne MyEthics.

Fait à Paris, le 1er novembre 2025

Président de BIOSerenity