

Procédure de recueil et de traitement des alertes professionnelles Groupe BRED

Emetteur	DRCCP	Actions
Création	Janvier 2018	
Mise à jour	Mai 2018	
Mise à jour	Mars 2020	MAJ Directeur des Risques de la Conformité et des Contrôles Permanents
Mise à jour	Novembre 2021	MAJ Directeur Conformité et Inspecteur Général
Mise à jour	Janvier 2022	MAJ outil d'alertes

SOMMAIRE

1. PREAMBULE	3
2. LES FAITS SUSCEPTIBLES D'ETRE SIGNALES	3
2.1. Les faits éligibles	3
2.2. Les exceptions à la faculté d'alerte prévue par la loi	4
3. LA DEFINITION DE LANCEUR D'ALERTE	4
4. LE DISPOSITIF DE RECUEIL DES ALERTES.....	4
4.1. L'émission d'une alerte.....	4
4.2. L'identification du lanceur d'alerte.....	5
4.3. Le formalisme requis	5
4.4. La réception d'une alerte	5
5. LE TRAITEMENT DES ALERTES	6
5.1. Les référents	6
5.2. La qualification des faits	6
5.3. Les garanties reconnues au lanceur d'alerte	7
5.4. Les garanties reconnues à toute autre personne éventuellement concernée	8
5.5. Utilisation abusive du dispositif	8
5.6. Les délais d'archivage	8
5.7. La durée de conservation des données à caractère personnel	9
5.8. Les mesures de sécurité	9

1. Préambule

La présente procédure cadre décline, sur le périmètre du Groupe BRED, la faculté d'alerte telle que prévue :

- par la loi 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi « Sapin II », ainsi que le Décret n° 2017-564 du 19 avril 2017 (applicable à toutes les entités, personnes morales du Groupe) ;
- par la loi du 27 mars 2017 relative au devoir de vigilance et la Directive (UE) 2019/1937 du Parlement européen du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union ;
- par l'article 37 de l'Arrêté du 03/11/2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ;
- ainsi que par l'ensemble des textes présents ou à venir, européens ou étrangers comportant un processus de recueil et de traitement d'alertes professionnelles.

La faculté d'alerte est complémentaire aux autres modes d'alerte de l'établissement. Chaque collaborateur a déjà la possibilité d'alerter sa ligne hiérarchique de toute interrogation de ce type. Pour les établissements bancaires, elle se distingue également des procédures obligatoires de déclaration, telles que, par exemple, les déclarations de soupçons auprès de TRACFIN ou les déclarations de soupçon sur les abus de marché, qui font l'objet de procédures spécifiques.

La faculté d'alerte a par définition un caractère optionnel. Son utilisation par les collaborateurs, dirigeants ou collaborateurs extérieurs et occasionnels ne revêt aucun caractère obligatoire, sauf pour les pays où la réglementation l'impose. A ce titre, aucune sanction ne pourra être prise à l'encontre d'un collaborateur au motif que ce dernier ou cette dernière n'en aurait pas fait usage.

2. Les faits susceptibles d'être signalés

2.1. Les faits éligibles

Les faits susceptibles de faire l'objet d'une alerte ou d'un signalement portent, sur :

- toute conduite ou situation qui serait contraire au code de conduite du Groupe BRED ;
- tout fait grave tel que :
 - un crime ou un délit, y compris des faits de corruption ou de trafic d'influence ;
 - une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ;
 - une violation grave et manifeste de la loi ou des textes d'application (décret, arrêté, règlement...);
 - une menace ou un préjudice grave pour l'intérêt général, dont l'émetteur a eu personnellement connaissance ;
- les atteintes graves envers les droits humains, en particulier la discrimination, l'atteinte à l'égalité, au respect de la vie privée, au droit de grève, à la liberté de réunion et d'association ainsi que l'atteinte des libertés fondamentales ; les atteintes à la santé et la sécurité des personnes (telles que le risque sanitaire), le non-respect des conditions de travail légales... ainsi que les risques liés à l'environnement ;
- tout risque d'impacts négatifs réels ou potentiels associés aux activités du groupe ou à ses relations d'affaires, envers les droits humains, les libertés fondamentales, la santé et la sécurité des personnes, l'environnement, au titre de la loi sur le devoir de vigilance.

Les informations communiquées devront porter sur des faits objectifs, matériellement vérifiables, susceptibles de faire apparaître la nature présumée des manquements éventuels. Seules seront prises en compte les données formulées de manière objective, pertinente, en adéquation et en rapport direct avec le champ d'application de la faculté d'alerte et strictement nécessaires aux vérifications ultérieures.

Tout écrit étant susceptible, dans le cadre d'une procédure judiciaire, d'être mis à la disposition des autorités, le lanceur d'alerte doit décrire les faits en toute objectivité, avec toute la rigueur et le professionnalisme qui s'imposent naturellement à un salarié ou un collaborateur externe et occasionnel, et de manière à ne pas prendre le risque d'engager l'entité, et plus généralement une entité du Groupe BRED, les dirigeants des entités et ses employés ou collaborateurs au-delà de leurs responsabilités. Le lanceur d'alerte doit adopter une formulation qui, d'une part, fasse apparaître le caractère présumé des faits, d'autre part, ne soit en aucun cas de nature à porter atteinte à la vie privée des collaborateurs ou dirigeants de l'entité ou du groupe, ou de tout tiers.

2.2. Les exceptions à la faculté d'alerte prévue par la loi

Les faits, informations ou documents couverts par :

- le secret de la défense nationale ;
- le secret médical ;
- le secret des relations entre un avocat et son client ;

ne peuvent être révélés.

3. La définition de lanceur d'alerte

Le lanceur d'alerte est cumulativement :

- une personne physique ;
- qui révèle de manière désintéressée et de bonne foi ;
- des faits éligibles ;
- dont elle a personnellement connaissance.

Pour l'application du présent chapitre, il convient de considérer le terme personne physique comme étant :

- un membre du personnel de l'entité ;
- ou un collaborateur extérieur et occasionnel (y compris dans le cas où sa société d'appartenance a mis en place son propre dispositif d'alerte professionnelle) incluant, à titre non limitatif :
 - les salariés mis à disposition par une entreprise extérieure ;
 - les intérimaires ;
 - les stagiaires écoles, les alternants ;
 - les consultants ou prestataires indépendants.

Ce dispositif est également mis à disposition des tiers en lien avec les activités du Groupe BRED et celles de ses sous-traitants ou fournisseurs pour les manquements liés au devoir de vigilance.

Il résulte de ce qui précède que n'est pas éligible au dispositif d'alerte de l'entité, une alerte qui serait émise par une personne physique sans lien de collaboration avec l'entité (exemple : un client de la banque), ce qui ne préjuge pas cependant de la pertinence de l'alerte qui pourra cependant faire l'objet d'un traitement en dehors du présent dispositif cadre.

4. Le dispositif de recueil des alertes

4.1. L'émission d'une alerte

L'alerte est portée à la connaissance des référents par le dépôt d'un signalement sur une plateforme sécurisée dédiée, accessible à l'adresse URL suivante :

<https://www.bkms-system.com/BRED>

Ce lien est accessible en permanence, à partir de n'importe quelle connexion (matériel téléphonique et informatique personnel ou fourni par l'entreprise). Il est unique pour tous les collaborateurs du Groupe BRED.

Le dispositif de recueil des alertes n'a pas pour objet de se substituer aux autres canaux d'alerte existants : hiérarchie directe ou indirecte, représentants du personnel etc. Il en est complémentaire. Il s'agit d'une faculté et non d'une obligation.

4.2. L'identification du lanceur d'alerte

L'identification du lanceur d'alerte est recommandée dans la mesure où, d'une part, le lanceur d'alerte peut alors bénéficier de toutes les garanties accordées par la loi, et d'autre part car son identification permet de traiter de la manière la plus efficace les défaillances ou déficiences signalées. La loi Sapin II ne stipule pas que le lanceur d'alerte soit obligatoirement identifié.

Un lanceur d'alerte souhaitant conserver l'anonymat devra bénéficier de la même protection définie au chapitre 5.3 s'il est ultérieurement identifié et fait l'objet de représailles. L'alerte est recevable et devra être comptabilisée 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.

Il faut distinguer le lanceur d'alerte de l'alerte en tant que telle. Si le lanceur d'alerte souhaite rester anonyme son alerte n'en reste pas moins recevable et ne doit pas faire l'objet d'un traitement différencié, ni d'un classement différencié.

4.3. Le formalisme requis

L'alerte comporte *a minima* :

- si l'émetteur de l'alerte ne souhaite pas conserver son anonymat : l'identité et les fonctions qu'il occupe ;
- l'identité, les fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- les éléments permettant le cas échéant un échange avec le destinataire du signalement ;
- les faits signalés, illustrant l'interrogation objet de l'alerte ;

complétée, le cas échéant, des informations et faits dont le lanceur d'alerte a personnellement connaissance.

4.4. La réception d'une alerte

Le destinataire de l'alerte doit :

- sans délai accuser réception de celle-ci auprès du lanceur d'alerte, en toute confidentialité ;
- s'assurer de l'éligibilité de l'alerte au dispositif prévu par la présente procédure.

A cet effet, il doit vérifier que :

- les faits révélés entrent dans la liste précisée au chapitre 2.1 et ne font pas l'objet d'une exception prévue au chapitre 2.2 ;
- le lanceur d'alerte est une des personnes prévues au chapitre 3 ;
- le formalisme attendu pour porter l'alerte à la connaissance du destinataire est respecté.

Dès lors que les prérequis sont cumulativement respectés, le destinataire de l'alerte informe, dans un délai qui ne peut être supérieur à 15 jours ouvrés après la réception de l'alerte, le lanceur d'alerte de la recevabilité de son alerte, par tout moyen permettant de garantir la stricte confidentialité de l'identité du lanceur d'alerte.

A défaut de respect des prérequis, le lanceur d'alerte est informé de la non-recevabilité de son alerte comme relevant du dispositif de protection du lanceur d'alerte, dans les mêmes conditions de délai et de confidentialité. L'alerte pertinente sera toutefois qualifiée par les référents.

5. Le traitement des alertes

5.1. Les référents

L'accès à l'outil de traitement des alertes professionnelles et au contenu des alertes est uniquement réservé aux référents que sont :

- Arnaud VIRICEL - Directeur des Risques de la Conformité et des Contrôles Permanents ;
- Didier LAIRIE - Directeur de la Conformité des Services d'Investissements ;
- Marie-Pierre SCIARA – Directeur de la Conformité.

Si le signalement concerne l'un des référents cités ci-dessus, il sera affecté par l'outil le cas échéant à :

- Aurélien PENNERAT – Directeur de l'Inspection Générale

5.2. La qualification des faits

Le traitement d'une alerte jugée recevable intervient dans un délai de 3 mois, à compter de sa réception, sans pour autant que ce délai ne constitue une limite pour assurer un traitement exhaustif de l'alerte.

Le destinataire de l'alerte ou les personnes spécialement chargées de la gestion des alertes professionnelles au sein de l'établissement ou, le cas échéant, des entités du Groupe BRED, évaluent le caractère de gravité de l'alerte au moyen d'une enquête, le cas échéant en s'appuyant sur les directions compétentes, tout en conservant secrète l'identité du lanceur d'alerte, sauf accord formel de ce dernier. Les informations recueillies par l'ensemble des destinataires du signalement sont également confidentielles. Un engagement de confidentialité sera signé par toute personne intervenant dans le traitement de l'alerte.

Lors de l'enregistrement de l'alerte, le lanceur d'alerte doit être informé que les informations recueillies feront l'objet d'un traitement informatique destiné à l'examen et l'analyse des données, que les destinataires des données sont les personnes spécialement chargées de la gestion des alertes professionnelles et que, conformément à la loi « informatique et libertés » du 6 janvier 1978, il bénéficie d'un droit d'accès et de rectification aux informations qui le concernent et qu'il peut exercer ce droit en s'adressant uniquement et directement au destinataire de l'alerte désigné au chapitre 5.1. Enfin, le déclarant est également informé qu'il peut, pour des motifs légitimes, s'opposer au traitement des données qui le concernent.

La personne en contact avec l'émetteur de l'alerte veille à ce que les informations transmises soient strictement en rapport avec les faits éligibles déclarés.

Le traitement des données portées à la connaissance des destinataires définis au chapitre 5.1 est effectué à l'aide de moyens dédiés reposant sur tous supports, informatisés ou non.

Seules les catégories de données suivantes peuvent être traitées :

- identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;
- identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- faits signalés, incluant potentiellement : données RH, données relatives au domaine bancaire, données relatives à la fraude... ;
- éléments recueillis dans le cadre de la vérification des faits signalés ;
- compte rendu des opérations de vérification ;
- suites données à l'alerte.

Les faits recueillis sont strictement limités aux actes visés par le dispositif d'alerte. La prise en compte de l'alerte professionnelle ne s'appuie que sur des données formulées de manière objective, en rapport

direct avec le périmètre du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués. Les formulations utilisées pour décrire la nature des faits signalés font apparaître leur caractère présumé.

Les alertes ainsi recueillies, y compris provenant des filiales en dehors de l'Union Européenne, peuvent être communiquées aux organes de direction, de contrôle et de surveillance du Groupe BRED ou d'une entité du Groupe BPCE le cas échéant, dans la mesure où ces données sont nécessaires à l'accomplissement de leur mission.

La direction de l'entité se réserve l'entière liberté d'appréciation des suites devant être données à l'exercice de la faculté d'alerte par un collaborateur, un dirigeant ou un collaborateur extérieur et occasionnel, dans le cadre des sanctions prévues dans le règlement intérieur de l'établissement.

Le lanceur d'alerte est informé des suites données à son alerte et, sans préjudice des garanties qui lui sont offertes dans le cadre de la procédure, peut être amené à présenter ses observations dans le cadre des procédures diligentées à la suite de l'alerte.

5.3. Les garanties reconnues au lanceur d'alerte

Aux conditions énoncées ci-dessus, le lanceur d'alerte bénéficie d'une protection légale, assurée de la manière suivante :

5.3.1.Des garanties de confidentialité

Le dispositif garantit une stricte confidentialité de l'identité du lanceur d'alerte, des personnes concernées et des informations recueillies, à toutes les étapes du traitement de l'alerte :

- le contenu de l'alerte professionnelle réalisée en ligne est protégé par un mot de passe ;
- tous les échanges entre le lanceur d'alerte et le Référent, de même que les enquêtes et rapports correspondants, sont confidentiels ;
- les personnes qui traitent des signalements (les Référents) sont en nombre restreint et sont toutes soumises à une obligation stricte de confidentialité ;
- le cas échéant, les experts missionnés dans le cadre de l'enquête s'engagent contractuellement à assurer la confidentialité des données liées à l'alerte professionnelle et à les supprimer au terme de leurs investigations ;
- les éléments de nature à identifier le lanceur d'alerte ne peuvent jamais être divulgués :
 - à la personne concernée par l'alerte, même si elle exerce son droit d'accès, au titre de la loi sur la protection des données ;
 - sans le consentement préalable du lanceur d'alerte, sauf à l'autorité judiciaire.

Les éléments de nature à identifier la personne physique et/ou morale mise en cause par un signalement ne peuvent pas être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

5.3.2.Une protection pénale

Pour mémoire, le fait de divulguer les éléments confidentiels relatifs au lanceur d'alerte et/ou à la personne physique et/ou morale mise en cause est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

Toute personne qui tenterait d'empêcher le lanceur d'alerte d'effectuer une alerte encourt une sanction pénale pour obstacle à la transmission d'une alerte.

Par ailleurs, n'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que les conditions suivantes sont cumulativement respectées :

- la divulgation des informations est nécessaire et proportionnée à la sauvegarde des intérêts en cause ;
- le signalement respecte la présente procédure et entre dans le champ d'application et du présent dispositif ;

- l'auteur du signalement répond aux critères de définition du lanceur d'alerte prévus à l'article 6 de la 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 (Article 122-9 du Code Pénal).

5.3.3. Une protection en droit du travail

Conformément à la loi, le Groupe BRED garantit l'absence de mesures disciplinaires ou de poursuites en lien avec le signalement aux conditions ci-dessus.

Le lanceur d'alerte est ainsi protégé contre toute mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération ou d'évolution professionnelle ou toute sanction disciplinaire et représailles qui seraient fondées sur le fait d'avoir signalé une alerte, dans le respect de la présente procédure.

5.4. Les garanties reconnues à toute autre personne éventuellement concernée

Lorsque l'interrogation met en cause directement ou indirectement une ou d'autres personnes, l'entité s'engage à assurer la collecte et le traitement des données les concernant dans des conditions conformes à la présente procédure, aux lois et règlements applicables et en particulier aux principes définis par la CNIL.

L'information de la personne concernée est assurée par la personne destinataire l'alerte, si cela est jugé nécessaire.

L'identité de la ou des personnes concernées par une interrogation est protégée par les mêmes règles de confidentialité que celles garanties à l'émetteur.

5.5. Utilisation abusive du dispositif

L'utilisation abusive de la faculté d'alerte, notamment lorsqu'elle vise une personne, peut exposer son auteur à d'éventuelles sanctions ou poursuites. Il est à cet égard rappelé que la dénonciation calomnieuse, définie comme celle effectuée de mauvaise foi par une personne qui connaît le caractère infondé de cette dénonciation, est pénalement sanctionnée par une peine pouvant atteindre 5 ans de prison et/ou 45 000€ d'amende aux termes de l'Article 226-10 du Code pénal.

5.6. Les délais d'archivage

Les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme n'entrant pas dans le champ du dispositif sont détruites ou archivées sans délai.

Lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les données relatives à cette alerte sont détruites ou archivées par l'organisation chargée de la gestion des alertes dans un délai de deux mois 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 par l'organisation chargée de la gestion des alertes 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.

5.7. La durée de conservation des données à caractère personnel

Les données à caractère personnel 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 conformément à l'avis 05/2014 relatif aux techniques d'anonymisation du Comité européen de la protection des données, et conservées pour une durée de deux ans suivants la clôture des opérations de vérification.

Lorsqu'aucune suite n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées par l'organisation chargée de la gestion des alertes, dans un délai de deux mois à compter de la clôture des opérations de vérification. Pour les besoins du présent référentiel, le terme « suite » désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agir de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services de la société, d'une sanction prononcée ou de la mise en œuvre d'une action en justice.

Lorsqu'une procédure disciplinaire et/ou des poursuites judiciaires sont engagées à l'issue des vérifications, les données relatives à l'alerte sont conservées jusqu'au terme de la procédure contentieuse. A l'issue d'une procédure disciplinaire et/ou des poursuites judiciaires, et après les éventuels délais de recours, seules les données relatives à l'alerte sont supprimées. Les données recueillies dans le cadre du contentieux sont conservées selon les délais d'archivage usuels.

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.

Le droit à l'oubli impose de ne pas conserver des données plus de 5 ans à compter de la clôture des opérations de vérification. Aussi, les données peuvent être conservées plus longtemps en archivage intermédiaire à condition d'être anonymisées ou si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).

5.8. Les mesures de sécurité

Le destinataire de l'alerte et les personnes spécialement chargées de la gestion des alertes professionnelles prennent toutes précautions utiles pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur communication ou de leur conservation. En particulier, les accès aux traitements de données s'effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification.

Ces accès sont enregistrés et leur régularité est contrôlée. L'identité de l'émetteur d'une alerte et des personnes visées par l'alerte ainsi que les informations recueillies par l'ensemble des destinataires du signalement sont traitées de façon confidentielle.