



DISPOSITIF DE RECUIEL ET TRAITEMENT DES ALERTES PROFESSIONNELLES OU « WHISTLE BLOWING »

Dans le cadre de son programme de « Compliance » et pour satisfaire à ses obligations légales, IBM France a mis en place un dispositif de recueil et traitement des signalements en application de la loi n°2016-1691 du 9 décembre 2016 telle que modifiée par la loi n° 2022-401 du 21 mars 2022 et son décret d'application n° 2022-1284 du 3 octobre 2022.

1. Quels sont l'objet et le champ d'application du dispositif ?

Ce dispositif permet de procéder à un signalement de faits qui se sont produits ou sont très susceptibles de se produire au sein de la société IBM France :

- Un crime ;
- Un délit ;
- Une menace pour l'intérêt général ;
- Une violation ou une tentative de violation :
 - D'un engagement international régulièrement ratifié ou approuvé par la France ;
 - D'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ;
 - Du droit de l'Union Européenne ;
 - De la loi ;
 - Du règlement.
 - De règles internes (code de conduite anticorruption d'IBM France ou Business Conduct Guidelines, etc)

Nous attirons votre attention sur le fait que :

- Vous devez avoir eu connaissance de ces faits dans le cadre de vos activités professionnelles ou, si vous en avez eu connaissance en dehors de votre cadre professionnelle, vous devez en avoir eu personnellement connaissance ;
- Vous devez être de bonne foi dans votre démarche ;
- Vous ne devez pas rechercher de contrepartie financière directe ;
- Les informations communiquées doivent être factuelles et présenter un lien direct avec l'objet de l'alerte ;
- Votre signalement ne doit pas concerner des faits, informations ou documents couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son

client, sauf si ceux-ci vous appartiennent, comme vos échanges avec votre avocat ou vos antécédents médicaux personnels.

2. Qui peut utiliser ce dispositif ?

Conformément aux dispositions légales, ce dispositif peut être utilisé par :

- Les membres du personnel de la société IBM France, lorsque les informations ont été obtenues dans le cadre de leur activité professionnelle ;
- Les personnes dont la relation de travail avec la société IBM France s'est terminée, lorsque des informations ont été obtenues dans le cadre de cette relation ;
- Les personnes qui se sont portées candidates au sein de la société IBM France, lorsque les informations ont été obtenues dans le cadre de cette candidature ;
- Les actionnaires, associés et titulaires de droits de vote au sein de l'assemblée générale la société IBM France ;
- Les membres des organes d'administration, de direction ou de surveillance la société IBM France ;
- Les collaborateurs extérieurs et occasionnels de la société IBM France ;
- Les cocontractants, sous-traitants de la société IBM France, étant précisé que s'il s'agit d'une personne morale, le signalement doit être émis par les membres de l'organe d'administration, de direction ou de surveillance ou par un membre de leur personnel.

3. Quelle est la procédure à suivre pour émettre un signalement ?

3.1. Les membres du personnel, ainsi que toute personne mentionnée au point 2 ayant accès à l'intranet, sont invités à suivre la procédure disponible sur l'intranet à l'adresse suivante

https://w3.ibm.com/hr/web/fr/erlr/alerte_professionnelle

et à émettre leur signalement via la plateforme « Employee Concerns » :

<https://w3.ibm.com/hr/employee-concerns/#/home/employee-concerns>

3.2. Les personnes mentionnées au point n'ayant pas accès à l'intranet, sont invités à procéder au signalement via les outils ci-dessous :

- Les fournisseurs peuvent émettre un signalement auprès de l'Ombudsman à l'adresse email suivante IBM.Ombudsman@ibm.com, disponible sur le site :
<https://www.ibm.com/procurement/ombudsman-information>
- Les Business Partners peuvent émettre un signalement auprès de Tell@IBM soit à l'adresse email suivante : tellibm@us.ibm.com, soit ou via ou disponible sur le site internet
<https://ibm.seismic.com/>
- Les autres personnes peuvent émettre un signalement à l'adresse email : trustww@us.ibm.com, disponible sur le site suivant :
<https://www.ibm.com/investor/governance/trust-and-compliance>

Conformément à l'article 1.3 des BCG et à la présente politique, tout signalement reçu par l'un des dispositifs susmentionnés ou par tout autre service ou personne, devra être redirigé auprès du dispositif dédié ou auprès du Référent signalement IBM France en cas d'erreur de l'émetteur du signalement sur le dispositif choisi.

3.3. Afin de permettre un meilleur traitement de votre signalement, nous vous remercions d'indiquer :

- ✓ La descriptions des faits objet du signalement ;
- ✓ Les dates précises et les lieux ;
- ✓ Les noms des personnes impliquées ainsi que les témoins éventuels ;
- ✓ Toute autre information permettant de vérifier et comprendre les faits objet du signalement ;
- ✓ Tous les éléments de preuve que vous aurez recueillis au soutien de votre signalement.

4. Comment se déroule le dispositif après mon signalement ?

Etape 1 : Réception et prise en charge du signalement par le dispositif saisi parmi ceux mentionné au point 3, lequel informera le Référent Signalement IBM France.

Etape 2 : Vous recevrez **un accusé de réception de votre signalement** dans un délai de **sept jours ouvrés** à compter de la réception du signalement.

Etape 3 : Examen de votre signalement pour vérifier qu'il remplit les conditions légales et réglementaires applicables relatives aux champ d'application matériel et à votre qualité d'émetteur

- Si votre signalement ne répond pas à ces conditions, vous en serez informé ainsi que si possible des autres voies disponibles pour permettre le traitement de l'objet de votre signalement
- Si votre signalement répond à ces conditions, il fera l'objet d'un traitement dans un délai raisonnable dans les conditions prévues par la loi (cf étape 4)

Etape 4 : Phase d'instruction de votre signalement

Etape 5 : A l'issue du traitement, vous serez informé par écrit des suites données à votre signalement, dans un délai n'excédant pas trois mois à compter de l'accusé de réception de votre signalement :

- Si les allégations sont inexactes ou infondées ou lorsque le signalement est devenu sans objet, vous serez informé de la clôture du dossier ;
- A défaut, vous serez informé, dans la mesure du possible, des mesures envisagées ou prises pour évaluer l'exactitude de vos allégations et, le cas échéant, remédier à l'objet du signalement ainsi que sur les motifs de ces dernières.

Au cours de la procédure, vous pourrez être contacté pour obtenir des informations complémentaires nécessaires au traitement du signalement, sous réserve que vous ayez communiqué vos coordonnées ou un autre moyen de vous contacter.

5. Puis-je utiliser le dispositif de façon anonyme ?

Le dispositif peut être utilisé de manière anonyme.

Si vous souhaitez rester anonyme, vous devez fournir des informations suffisantes pour permettre le traitement du signalement tout en évitant de fournir des éléments permettant de vous identifier et donner un moyen de vous contacter afin de pouvoir fournir, au besoin, des informations complémentaires.
Si l'anonymat rend impossible le traitement du signalement, vous en serez informé dans la mesure du possible.

IBM France se réserve le droit de ne pas traiter les signalements anonymes si la gravité des faits remontés n'est pas établie ou si les éléments factuels ne sont pas suffisamment détaillés, sans possibilité de vous contacter pour obtenir plus d'information

6. Quelles sont les garanties du traitement de mon signalement ?

Plusieurs garanties sont mises en œuvre dans le cadre des dispositifs de signalement, dans le respect des dispositions légales et réglementaires applicables :

- ✓ Les signalements feront l'objet d'un traitement objectif, impartial, dans le respect du principe de la présomption d'innocence et de bonne foi.
- ✓ Les signalements sont traités par des personnes dédiées soumises à une obligation de stricte confidentialité dans le traitement des signalements.
- ✓ Les moyens mis à disposition permettent également l'impartialité et la confidentialité du traitement du signalement.
- ✓ Le dispositif mis en œuvre interdit l'accès aux informations aux personnes non habilitées ;
- ✓ Les informations recueillies ne pourront être transmises à des tiers que si cette communication est nécessaire au traitement et dans le respect des dispositions applicables.

7. Suis-je obligé d'utiliser ce dispositif ?

IBM France encourage à utiliser en priorité le dispositif interne de signalement objet des présentes.

Cependant, vous pouvez choisir de procéder à un signalement externe, soit après un signalement par le biais des dispositifs internes, soit directement auprès :

- Des autorités compétentes dont la liste est fixée en annexe du Décret n° 2022-1284 du 3 octobre 2022, chacune disposant d'un dispositif propre ;
La liste est disponible sur le lien ci-dessous :
<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT00004635736>
8
- Du Défenseur des droits ;
- De l'autorité judiciaire ;
- D'une institution, d'un organe ou d'un organisme de l'Union Européenne compétent.

8. Est-ce que je prends un risque à effectuer un signalement via ce dispositif ?

Une utilisation de bonne foi, sans intention de nuire, du dispositif de signalement n'est pas susceptible de sanctions ou de toute autre mesure de représailles ainsi que toute menace ou tentatives de représailles, conformément à la politique interne d'IBM en la matière.

L'utilisation de bonne foi suppose la transmission d'informations complètes et loyales telles que vous pouviez raisonnablement croire en leur véracité au moment de l'émission de l'alerte.

Seule une utilisation abusive ou à des fins intéressées sera susceptible de donner lieu à des sanctions disciplinaires ou des poursuites judiciaires.

Les dispositions légales et réglementaires ont mis en place un dispositif protecteur spécifique pour les lanceurs d'alerte au sens de la loi n°2016-1691 du 9 décembre 2016, lequel suppose de remplir des conditions précises. Sur ce point, l'utilisation de ce dispositif et l'éventuelle décision de recevabilité ne valent pas reconnaissance du bénéfice éventuel ou non de lanceur d'alerte, qu'il vous appartient de vérifier.

Il est rappelé que cette protection peut, sous réserve d'en remplir les conditions, s'appliquer également :

- Aux facilitateurs, entendus comme toute personne physique ou personne morale de droit privé à but non lucratif qui aide un lanceur d'alerte à effectuer un signalement ou une divulgation dans le cadre du présent dispositif ;
- Aux personnes physiques en lien avec un lanceur d'alerte au sens de la loi n°2016-1691 du 9 décembre 2016, qui risquent de faire l'objet de représailles dans le cadre de leurs activités professionnelles de la part de leur employeur, de leur client ou du destinataire de leurs services ;
- Aux entités juridiques contrôlées, au sens de l'article L.233-3 du code de commerce, par un lanceur d'alerte au sens de la loi n°2016-1691 du 9 décembre 2016, pour lesquelles il travaille ou avec lesquelles il est lié dans un contexte professionnel.

* *
*