Baker Tilly au Luxembourg
Lignes directrices du système de lancement d'alerte

Introduction : qu'est-ce que le lancement d'alerte, et pourquoi est-ce important ?

Baker Tilly au Luxembourg, composé des entités suivantes:

- Baker Tilly Luxembourg Experts-Comptables S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Corporate Services S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Advisory S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Training S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Innovation S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Interaudit S.à r.l., 37, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Audit & Assurance s.à r.l., 2, rue Peternelchen, L-2370 Howald, Luxembourg,
- Fibetrust S.à r.l., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,

(ci-après désignées collectivement par « Baker Tilly ») s'efforce d'allier transparence et haut niveau d'éthique professionnelle. C'est dans cette optique que Baker Tilly a mis en place cette procédure interne ainsi qu'un canal interne de lancement d'alerte, offrant aux employés et prenantes externes la possibilité de signaler de manière confidentielle tout soupçon de conduite inacceptable. Comme développé dans le reste du document, le lancement d'alerte peut être effectué de manière confidentielle ou anonyme.

Ce document s'inscrit dans le cadre de la conformité à la législation luxembourgeoise relative au lancement d'alerte (Loi du 16 mai 2023 portant transposition de la Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union) ainsi qu'à la législation sur la protection des données personnelles (Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques).

Quand lancer une alerte ?

Notre service de lancement d'alerte peut être utilisé pour prévenir de risques sérieux vous affectant ou vos collègues ou tout autre individus, ainsi que l'organisation. Les problèmes signalés peuvent inclure des délits, des irrégularités, des violations ou d'autres actions contraires aux lois européennes ou nationales, dans un **contexte professionnel**, tels que :

- ✓ ***Corruption et irrégularités financières*** *; par exemple, pots-de-vin, concurrence déloyale, blanchiment d'argent, fraude, conflit d'intérêts.*
- ✓ ***Violations en matière de santé et de sécurité ;*** *par exemple, santé et sécurité sur le lieu de travail, sécurité des produits, discrimination grave et harcèlement qui vont tous à l'encontre de la loi.*
- ✓ ***Violations en matière d'environnement ;*** *par exemple, traitement illégal de déchets dangereux.*
- ✓ ***Violations de la vie privée ;*** *par exemple, utilisation abusive de données personnelles.*

Veuillez noter que ce service de signalement interne n'est pas approprié pour soulever tout grief personnel lié à vos conditions de travail, à votre évaluation de performance ou à toute autre préoccupation similaire. Nous vous invitons pour cela à discuter de votre préoccupation avec votre responsable.

Une personne qui lance l'alerte n'a pas besoin de disposer de preuves irréfutables pour exprimer un soupçon. Cependant, le signalement délibéré d'informations fausses ou diffamatoires est pénalisé. Tout abus du service de lancement d'alerte constitue une infraction grave passible de sanctions disciplinaires.

Comment lancer l'alerte ?

Lancer l'alerte via la messagerie anonyme ou confidentielle par le biais du canal de signalement des lanceurs d'alerte à l'équipe chargée des lanceurs d'alerte : https://bakertillylux.integrity-speakingup.com/fr/home. Le lien est disponible sur notre site internet et la plateforme est accessible en scannant le code QR ci-dessous:

Vous pouvez soumettre votre signalement en remplissant un questionnaire sur le site web. Cette démarche peut être effectuée depuis votre ordinateur ou votre smartphone. Veuillez vous référer au lien ci-dessus pour toute information complémentaire sur l'utilisation de la plateforme.

Si vous avez suivi les étapes ci-dessus pour lancer une alerte mais estimez que la question n'a pas été résolue de manière satisfaisante, en conformité avec les obligations légales et dans un délai de 3 mois, vous pouvez adresser un rapport directement à l'autorité compétente. Dans ce cas, vous pouvez contacter le Reporting Office (13, rue Erasme, Centre administratif Werner, L-1468 Luxembourg, Tel: (+352) 247-88564), ou par email à l'adresse suivante : ods.info@mj.etat.lu pour

obtenir des informations générales sur l'autorité compétente en fonction du type de signalement concerné.

La procédure d'investigation

L'ÉQUIPE D'INVESTIGATION

L'accès aux messages reçus via le canal de signalement est limité aux individus désignés, chargés de gestion des cas d'alerte. Leurs actions sont tracées dans le journal d'événements et le traitement des alertes est strictement confidentiel. Conformément à ce qui précède, notre organisation a mandaté comme « équipe de gestion des alertes » une société de conseil externe et indépendante (« Grant Thornton Advisory ») pour être principalement responsable de la gestion de la plateforme et de tout signalement.

Quand cela est nécessaire, des experts - « investigateurs » - seront invités à intervenir sur la plateforme pour mener l'enquête. Ces personnes peuvent accéder aux données pertinentes telles que vous les avez partagées et sont également tenues de respecter strictement la confidentialité et/ou l'anonymat.

GESTION D'UN MESSAGE REÇU

Lors de la réception d'un message d'alerte, l'équipe de gestion des alertes décide d'accepter ou de rejeter le message. Si le message est accepté, des mesures d'enquête appropriées sont mises en œuvre. Veuillez consulter à ce propos la section « Enquête » ci-dessous. Le lanceur d'alerte doit recevoir un accusé de réception de son rapport dans un délai de 7 jours, et l'équipe d'investigation doit revenir vers l'auteur avec une réponse dans un délai de 3 mois à compter de la date de réception de l'alerte.

L'équipe d'investigation peut refuser l'alerte selon les conditions suivantes (non cumulatives) :

- ✓ le comportement signalé ne constitue pas un cas de lancement d'alerte selon ces directives de signalement ;
- ✓ le message n'a pas été rédigé de bonne foi, ou est malveillant ;
- ✓ il n'y a pas suffisamment d'informations pour mener une enquête ;
- ✓ l'objet du message a déjà été traité.

ENQUÊTE

Tous les messages sont traités avec sérieux et avec un strict respect des règles de confidentialité décrites dans ces directives sur le signalement.

- ✓ Aucune personne au sein de l'équipe d'investigation, et aucune personne participant à une enquête, ne doit pas rechercher à identifier la personne qui effectue un signalement.
- ✓ L'équipe d'investigation peut, si nécessaire, soumettre des questions de suivi, par le biais du canal de communication anonyme.
- ✓ L'enquête sur une alerte ne sera jamais confiée à une personne susceptible d'être impliquée dans, ou liée à la question soulevée.
- ✓ Des experts interne à l'entreprise ou externes peuvent être inclus dans l'enquête avec le consentement du lanceur d'alerte.

Si une personne fait l'objet d'une enquête, elle en sera informée en temps utile, à moins que cela ne nuise gravement à l'enquête ou que le retard dans la notification soit autrement justifié.

Protection de la vie privée

PROTECTION DES LANCEURS D'ALERTES

Une personne qui signale un véritable soupçon ou inquiétude ne doit pas risquer de perdre son emploi ni de subir quelque forme de représailles ou de désavantage personnel ou professionnel que ce soit. Le lanceur d'alerte ne doit pas être sanctionné pour avoir soulevé une alerte ou un soupçon, tant qu'il agit de bonne foi.

Sous réserve du respect du droit à la protection des données personnelles des personnes faisant l'objet de signalements, les lanceurs d'alerte identifiés doivent être informés des suites de l'enquête.

En cas de signalement de délits présumés, la personne à l'origine du signalement est informée sous condition de son **consentement**, que son identité pourrait être divulguée aux autorités judiciaires.

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Ce service d'alerte professionnelle peut collecter des données personnelles sur la personne mise en cause dans un message, le déclarant qui envoie le rapport (s'il n'est pas envoyé de manière anonyme) et toute tierce personne impliquée, afin d'enquêter sur les faits relatifs aux manquements rapportés et aux comportements inappropriés relevant de notre code de conduite ou de nos règles internes. Ce traitement peut être fondé sur l'obligation légale ou notre intérêt légitime de prévenir les risques liés à la réputation et de promouvoir une activité éthique. La description et les faits fournis dans le cadre de ce traitement sont uniquement réservés aux personnes compétentes et autorisées qui traitent ces informations de manière confidentielle. Vous pouvez exercer vos droits d'accès, de rectification et d'opposition, ainsi que de limitation de traitement de vos données à caractère personnel conformément à la législation locale en matière de protection des données. Ces droits sont soumis aux mesures de protection et de sécurité nécessaires pour éviter la destruction de preuves ou d'autres entraves au traitement et à une enquête sur le dossier. Pour toute autre question ou plainte, Veuillez adresser votre demande à notre équipe de protection des données, joignable à l'adresse suivante : dataprotection@bakertilly.lu.

SUPPRESSION DES DONNEES

Les données personnelles contenues dans les signalements et la documentation d'enquête sont supprimées une fois l'enquête terminée, sauf lorsque leur conservation est nécessaire en vertu de la législation applicable. L'outil permet la suppression définitive des dossiers 30 jours après la clôture de l'enquête. Les pièces jointes à l'enquête et les signalements archivés sont à anonymiser selon les règles de RGPD ; les messages archivés doivent exclure des données personnelles permettant l'identification de personnes de manière directe ou indirecte.

RESPONSABLE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL :

Baker Tilly est responsable des données à caractère personnel traitées dans le cadre du service d'alerte professionnelle.

SOUS-TRAITANTS DES DONNÉES À CARACTÈRE PERSONNEL :

WhistleBox BV (3290 Diest, Statiestraat 41, registered in the Crossroads Bank for Enterprises under number 0754.832.521) et Grant Thornton Advisory agissent en tant que sous-traitant pour les traitements de données réalisés pour le compte et sur instructions de Baker Tilly (responsable de traitement). Ni WhistleBox ni Grant Thornton Advisory ne sont en mesure de déchiffrer ou de lire les messages transmis de manière anonyme.