
POLITIQUE DE DÉNONCIATION

thinkproject

Conformité

Système de Management : Conformité

Produits : TOUS

ID du Document : CMS_0004

Version : 1.1

Classification : Ouvert

Créé par	Peter Mezger	15.07.2022
Approuvé par	Markus Scheuermann	15.07.2022
Date d'émission originale	29.07.2021	

Veillez ne pas imprimer de copie de ce document.

TABLE DES MATIÈRES

1	Résumé	3
2	Périmètre	3
3	Contenu de la Politique	4
4	Confidentialité et Protection des Données.....	5
5	IT and Data Security.....	5
6	Suppression des Données.....	5
7	Contrôle des Documents.....	6

Politique de Dénonciation

Système de Management : Conformité | Produits : TOUS

ID du Document : CMS_0004 | Version : 1.1 | Classification : Ouvert

Créé : 15.07.2022 | Approbation : 15.07.2022

1 RÉSUMÉ

Le système de dénonciation de Thinkproject est destiné à permettre aux employés et à d'autres personnes de soumettre des rapports anonymes. Le système d'alerte est destiné à enregistrer ces rapports selon un processus facilement compréhensible qui garantit la meilleure protection possible des intérêts légitimes des personnes concernées. Le système d'alerte vise à prévenir à la fois un préjudice financier pour l'entreprise et une perte d'image.

La dénonciation n'est prévue que pour les catégories suivantes de violations de règles qui sont / peuvent être pertinentes ou proches du droit pénal :

- conflits d'intérêts,
- corruption et pots-de-vin,
- droit des contrats publics,
- services financiers, produits financiers et marchés financiers,
- prévention du blanchiment d'argent et du financement du terrorisme,
- sécurité et conformité des produits,
- protection de l'environnement,
- sécurité des aliments et de la nutrition animale,
- santé,
- protection de la vie privée et des données personnelles
- sécurité des réseaux et des systèmes d'information
- droit de la concurrence
- 10 principes du Pacte mondial des Nations unies

Cette politique de dénonciation vise également à garantir, d'un point de vue technique et organisationnel, que les signalements de violations des lois, du Code de Conduite ou des lignes directrices sont reçus conformément aux exigences du Code de Conduite et à la confidentialité et la sécurité des données. Et qu'ils sont traités, stockés et archivés avec la confidentialité nécessaire.

Si les réglementations locales sont plus strictes que les normes minimales fixées par la présente directive, les règles les plus strictes s'appliquent dans chaque cas. S'il existe un conflit entre les lois pertinentes et la présente directive, la partie concernée doit en informer le responsable de la conformité afin de résoudre le conflit.

2 PÉRIMÈTRE

Cette politique s'applique à tous les dirigeants, administrateurs, employés, travailleurs contractuels et temporaires dans tous les lieux du monde et à tous les représentants de la société, y compris les consultants et les agents.

Politique de Dénonciation

Système de Management : Conformité | Produits : TOUS

ID du Document : CMS_0004 | Version : 1.1 | Classification : Ouvert

Créé : 15.07.2022 | Approbation : 15.07.2022

3 CONTENU DE LA POLITIQUE

OBLIGATION DE SIGNALER

Tout employé et toute autre personne du groupe Thinkproject sont autorisés à soumettre des rapports. Peu importe qu'ils soient employés d'une société du groupe Thinkproject ou d'une filiale d'une société du groupe Thinkproject.

Dans les limites autorisées par la loi et dans la mesure où cela est compatible avec la conduite d'une enquête adéquate, l'entreprise protégera la confidentialité et l'anonymat de la personne qui fait le rapport.

Cette politique n'implique aucune obligation pour quiconque de faire un rapport. Cependant, s'il existe des devoirs ou des obligations légales, contractuelles ou autres de fournir des rapports, ceux-ci ne sont pas affectés par le paragraphe ci-dessus.

PAS DE REPRÉSAILLES

Les employés et les autres personnes qui signalent un incident ne seront pas harcelés, ne subiront pas de représailles et ne subiront pas de conséquences négatives sur le plan de l'emploi, telles que le licenciement, la rétrogradation, la suspension, la discrimination en ce qui concerne les conditions d'emploi. Toutefois, les employés et les personnes associées qui exercent des représailles à l'encontre d'une personne ayant signalé un incident de bonne foi feront l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement.

SOUSSIONS DES RAPPORTS

La soumission de rapports sur des violations réelles ou présumées est rendue possible de la manière décrite ci-dessous :

- Les rapports peuvent être signalés de manière confidentielle au superviseur direct ;
- Les rapports peuvent être signalés directement et confidentiellement au département de conformité ;
- Les rapports peuvent être signalés directement via le système numérique d'alerte.

Dans le système d'alerte numérique, les formes des rapports sont techniquement prédéfinies. Dans tous les autres cas, cependant, la soumission des rapports n'est pas liée à un format spécifique. Un aperçu actualisé des canaux de signalement est disponible sur le lien suivant : <https://thinkproject.integrityline.com/> .

RAPPORTS PERTINENTS

Le système d'alerte est uniquement destiné à recevoir et à traiter les rapports relatifs à toute violation présumée ou réelle des lois, des politiques ou du Code de Conduite. Il n'est pas disponible pour les plaintes générales ou les demandes de renseignements sur les produits et les garanties.

Seuls doivent être soumis les rapports pour lesquels le dénonciateur croit de bonne foi que les informations qu'il a fournies sont correctes. En revanche, la personne n'est pas de bonne foi si elle sait qu'un fait signalé est faux. En cas de doute, les faits correspondants ne sont pas présentés comme un fait mais comme une hypothèse, une évaluation ou une déclaration d'autres personnes.

Il est à noter qu'un dénonciateur peut faire l'objet de poursuites si, en tout état de cause, il allègue des faits inexacts concernant d'autres personnes.

Politique de Dénonciation

Système de Management : Conformité | Produits : TOUS

ID du Document : CMS_0004 | Version : 1.1 | Classification : Ouvert

Créé : 15.07.2022 | Approbation : 15.07.2022

PROTECTION DU DÉNONCIATEUR

Tous les rapports, y compris les références au dénonciateur, seront traités de manière confidentielle et conformément aux lois applicables.

RESTRICTIONS LÉGALES

Dans certains pays, la législation prévoit certaines restrictions pour les signalements, par exemple, ce qui peut être signalé, si les données personnelles d'un individu peuvent être stockées, ou si les signalements peuvent être faits de manière anonyme. Les exigences correspondantes sont intégrées dans le système de dénonciation numérique. Toute préoccupation qui ne peut être signalée à l'aide des procédures de signalement mentionnées en raison de telles restrictions doit être adressée au supérieur hiérarchique de l'employé. Si un employé estime qu'il n'est pas possible de soulever la question au niveau local, il doit la transmettre au sein du département des Ressources Humaines local ou au département de conformité.

4 CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

Tous les rapports, quelle que soit leur véracité, sont susceptibles de nuire à la réputation des personnes concernées, des dénonciateurs et/ou des tiers, et de l'entreprise.

Nous les traitons donc avec confidentialité, au-delà des obligations découlant des lois sur la protection des données. En plus du registre des responsables du traitement des données, qui doit toujours être tenu à jour, il faut tenir un registre écrit des personnes susceptibles de travailler avec des données connexes et des droits dont elles disposent dans le cadre du traitement des données. Ces personnes doivent être tenues de respecter une confidentialité particulière au-delà des exigences légales.

5 IT AND DATA SECURITY

Les solutions informatiques pour la saisie et le traitement des rapports doivent être approuvées par le responsable de la sécurité de l'information, le responsable de la conformité et le délégué à la protection des données du groupe avant d'être utilisées. Les exigences minimales relatives au champ d'application du règlement général sur la protection des données découlent de l'art. 32 du GDPR, des directives du groupe en matière de sécurité informatique et de protection des données. La sensibilité des informations et les risques pour les personnes et l'entreprise si les données relatives à ces informations venaient à être connues doivent être considérés de manière appropriée. Le traitement efficace et effectif des rapports est garanti ainsi que la plus stricte confidentialité, notamment l'anonymat du collaborateur, pour les rapports de toute nature.

6 SUPPRESSION DES DONNÉES

L'effacement des données dans le système d'alerte numérique doit être effectué exclusivement conformément aux spécifications temporelles respectives du concept de suppression ou après approbation de suppression par deux utilisateurs distincts (principe des quatre yeux).

Politique de Dénonciation

Système de Management : Conformité | Produits : TOUS

ID du Document : CMS_0004 | Version : 1.1 | Classification : Ouvert

Créé : 15.07.2022 | Approbation : 15.07.2022

7 CONTRÔLE DES DOCUMENTS

Version	Date	Auteur	Approuvé par	Details des modifications apportées
001	17.06.21	Peter Mezger	Ralf Grüßhaber	Première version
1.1	15.07.22	Peter Mezger	Markus Scheuermann	Expansion Section 1

Politique de Dénonciation

Système de Management : Conformité | Produits : TOUS

ID du Document : CMS_0004 | Version : 1.1 | Classification : Ouvert

Créé : 15.07.2022 | Approbation : 15.07.2022
