Nom de la pratique:

Outil de lancement d'alertes

Pays:

Autriche

Catégorie de la pratique:

- Systèmes et outils

Contact:

- Ministère public chargé de la lutte contre la criminalité économique et la corruption
- www.justiz.gv.at/wksta/
- Tél. +43 1 526 36 86

Lutte contre les risques de fraude suivants:

- Conflit d'intérêts
- Contournement ou manipulation des procédures de passation de marchés publics
- Double financement
- Collusion
- Manipulation des coûts de projet
- Autres

Contexte et objectifs

Le ministère public autrichien chargé de la lutte contre la criminalité économique et la corruption a lancé en 2013 un outil de lancement d'alertes dans le cadre de la lutte contre la corruption. Cet outil comprend une messagerie qui permet de communiquer avec le lanceur d'alerte afin de lui demander des éclaircissements. Après une première phase d'essai, le système est en place de manière permanente depuis 2016 et un paragraphe sur le système et sur sa mission a été inclus dans la loi (§ 2a Abs 6 StAG).

Bien souvent, les structures criminelles ne peuvent être mises au jour que si le lanceur d'alerte bénéficie d'une protection suffisante contre les conséquences négatives. L'outil de lancement d'alertes garantit l'anonymat du lanceur d'alerte et favorise le signalement de la criminalité économique.

L'objectif de l'outil est de permettre aux enquêteurs du ministère public prendre directement contact avec les lanceurs d'alerte. Cette démarche améliore l'efficacité des poursuites pénales.

Description de la pratique

L'outil est conçu pour être un système de messagerie anonyme utilisant le système BKMS de Business Keeper (**https://www.business-keeper.com/fr/**), l'un des principaux fournisseurs de systèmes de lancement d'alertes dans l'UE.

Il invite les citoyens à signaler les actes suspects dont ils sont témoins dans leur environnement professionnel ou privé au moyen d'un lien affiché sur le site web du ministère fédéral de la justice. La mise en œuvre technique du système garantit l'anonymat de la source des informations. Les lanceurs d'alerte peuvent décider de rester anonymes ou de divulguer leur identité aux enquêteurs.

S'il subsiste des questions dans le chef des enquêteurs à la lecture des informations fournies, ceux-ci peuvent contacter directement le lanceur d'alerte grâce à une messagerie électronique dans l'outil. L'identité du lanceur d'alerte reste protégée tout au long du processus.

Les procureurs ont désormais la possibilité de demander des informations complémentaires qui peuvent servir à corroborer les allégations et mener éventuellement à l'ouverture d'une enquête, ce qui n'est pas possible avec les informations anonymes reçues par voie postale ou par d'autres canaux.

Les informations peuvent être soumises dans plusieurs des catégories spécifiques conformes au code pénal autrichien:

- corruption,
- criminalité financière,
- fraude à l'aide sociale,
- pratiques comptables frauduleuses,
- infractions sur les marchés financiers, et
- blanchiment de capitaux.

Le processus de lancement d'alerte passe par quatre étapes. Le lanceur d'alerte:

1. est invité à lire les informations relatives à la protection de son identité;
2. choisit la catégorie principale de signalement dans une liste (corruption, criminalité financière, fraude à l'aide sociale, pratiques comptables frauduleuses ou infractions sur les marchés financiers et blanchiment de capitaux);
3. décrit la situation dans ses propres termes et répond à une série de questions prédéfinies, par exemple concernant le préjudice subi et le lieu de l'incident (il est également possible de télécharger des documents);
4. est invité à créer un compte de messagerie pour communiquer avec les enquêteurs.

L'étape 4 n'est pas obligatoire pour faire un signalement, elle est facultative après les trois premières étapes mentionnées ci-dessus.

Il est également demandé spécifiquement au lanceur d'alerte s'il souhaite rester anonyme. Il peut aussi choisir d'être considéré comme un témoin clé s'il est impliqué dans l'infraction signalée.

Il est rappelé à la personne que les informations et les documents fournis pourraient conduire à son identification et qu'elle doit donc être particulièrement vigilante, notamment lors du choix du pseudonyme de son compte de messagerie ou en ne mentionnant pas ses liens avec l'accusé dans sa description de l'affaire. L'outil met en garde contre l'utilisation d'un ordinateur de travail pour effectuer le signalement.

Lorsqu'il a effectué le signalement, le lanceur d'alerte reçoit un numéro de référence à titre de confirmation.

Le signalement est transmis au ministère public, où quatre procureurs spécifiquement formés traitent actuellement les signalements reçus. En plus de leur expertise de procureurs, les enquêteurs ont dans un premier temps été formés au fonctionnement du système BKMS par Business Keeper et suivent régulièrement des cours sur des sujets connexes, tels que la communication avec le lanceur d'alerte.

Lorsqu'ils communiquent avec le lanceur d'alerte, les enquêteurs conservent également leur anonymat afin de bénéficier de la même protection.

Chaque signalement est analysé par deux procureurs, ce qui permet un examen selon le principe du double regard. Le ministère public peut immédiatement prendre les mesures qui s'imposent ou transmettre le signalement à un autre service si la situation ne relève pas de sa compétence. Si le signalement est jugé sérieux, le ministère public ouvre une enquête. Si le signalement ne nécessite pas que des mesures soient prises, le dossier est clôturé.
Le lanceur d'alerte est informé de la suite de la procédure sans recevoir d'informations détaillées. L'identité des lanceurs d'alerte n'étant pas connue, ceux-ci pourraient ne pas être en droit de recevoir des informations sur l'enquête, par exemple sur les victimes potentielles.

Le système BKMS est également un système de gestion des dossiers. Tous les documents et communications relatifs à un signalement sont stockés de manière sécurisée et électronique dans le système. Si une enquête est ouverte, les informations la concernant peuvent être facilement transmises.

L'outil est amélioré en permanence, par exemple en adaptant les informations mises à la disposition du lanceur d'alerte et en facilitant l'utilisation du système par les enquêteurs.

Caractéristiques uniques

- Anonymat du lanceur d'alerte
- Possibilité de communiquer avec le lanceur d'alerte au moyen d'une boîte de messagerie dans le système
- Communications cryptées
- Accès strictement réservé à l'équipe dédiée au sein du ministère public; accès impossible pour le fournisseur, Business Keeper, et pour tout autre tiers
- Absence de stockage des informations techniques concernant le lanceur d'alerte (par exemple, l'adresse IP)
- Système accessible 24 heures sur 24 et 7 jours sur 7, partout dans le monde
- Multiples rappels aux lanceurs d'alerte pour qu'ils ne divulguent, dans leur signalement, aucune information susceptible de conduire à leur identification s'ils souhaitent rester anonymes

Résultats

Depuis le lancement de l'outil, le système judiciaire autrichien est beaucoup plus vigilant: il reconnaît la nécessité de tenir compte des lanceurs d'alerte et de les motiver depuis que des cas graves de corruption sont récemment survenus en Autriche.

Fin 2019, le site web avait été consulté plus de 600 000 fois, avec environ 300 visites quotidiennes en moyenne. 9 345 signalements ont été effectués et, dans 6 210 cas, le lanceur d'alerte a utilisé la possibilité de créer une boîte de messagerie pour poursuivre la communication.

679 enquêtes ont été ouvertes sur la base des signalements reçus. 66 chefs d'accusation ont été portés devant les tribunaux. Les informations reçues dans le cadre de 48 signalements étaient inédites. 93 signalements ont été utilisés dans le cadre de procédures en cours.

Les signalements ont été répartis entre les catégories suivantes:

- 17,02 % pour la corruption,
- 19,45 % pour la fraude à l'aide sociale,
- 16,82 % pour la criminalité financière,
- 22,21 % pour la criminalité fiscale,
- 0,62 % pour les pratiques comptables frauduleuses et les infractions sur les marchés financiers, et
- 2,49 % pour le blanchiment de capitaux;
- 21,39 % dans la catégorie «autres», qui comprend les dossiers ne relevant pas des domaines mentionnés ci-dessus.

Facteurs clés de succès

- Garantie de l'anonymat des lanceurs d'alerte.
- Coopération avec des fournisseurs d'outils expérimentés.
- Formation des procureurs chargés des signalements.
- Communication sur la mise en œuvre de l'outil dans les médias et sur le site web du ministère public.

Difficultés rencontrées et enseignements tirés

- La base juridique (un paragraphe de la loi) est essentielle pour encourager les signalements et garantit que les informations peuvent être utilisées dans le cadre de procédures judiciaires.
- La coopération avec un fournisseur d'outils qui a fait ses preuves est un gage de sécurité dans le traitement des données et de structure dans la gestion des dossiers.
- Une communication appropriée sur l'existence et l'utilisation de l'outil ainsi que sur le traitement des informations est essentielle pour encourager les signalements.

Potentiel de transférabilité

- D'autres pays/autorités peuvent facilement adopter un système conçu par le même fournisseur d'outils, ou par un fournisseur similaire.
- Compte tenu de l'adoption de la directive sur la protection des personnes dénonçant les infractions au droit de l'Union (également connue sous le nom de directive sur les lanceurs d'alerte), qui impose à tous les États membres d'établir un canal de signalement des infractions, cette pratique pourrait servir d'orientation (la directive doit être transposée dans le droit national d'ici décembre 2021).
- La garantie de l'anonymat n'est pas juridiquement possible dans tous les États membres.