



DOUANE · CONFORMITÉ · IT

NOTE D'INFORMATION RÉGLEMENTAIRE

AEO : coopérer avec la douane face au trafic illicite

La nouvelle guidance de la Commission européenne, publiée le 14 avril 2026 : détecter, signaler et réagir aux activités suspectes. Ce qui change concrètement pour les opérateurs économiques agréés — et pour tous les acteurs de la chaîne logistique.

Guidance document — Commission européenne, DG TAXUD

« AEO — Customs Cooperation to Detect, Report and React to Suspicious Activities » · document du 31 mars 2026 (TAXUD/A3/002/2026), publié le 14 avril 2026

Édition août 2026

customs-conformit.be

AU SOMMAIRE

1. L'essentiel en un coup d'œil
2. Pourquoi cette guidance ?
3. Qui est concerné ?
4. Les obligations qui existent déjà
5. Les signaux d'alerte à reconnaître
6. Comment signaler : à qui, quand, quoi
7. Ce que vous pouvez attendre de la douane
8. Votre plan d'action et notre accompagnement
9. Modèle de fiche de signalement

1. L'essentiel en un coup d'œil

Le 14 avril 2026, la Commission européenne (DG TAXUD) a mis en ligne une nouvelle guidance : « **AEO — Customs Cooperation to Detect, Report and React to Suspicious Activities** », document daté du **31 mars 2026** (réf. TAXUD/A3/002/2026). Son objet : organiser un **échange d'informations à double sens** entre les douanes et les entreprises pour détecter et contrer le **trafic illicite**, le trafic de drogue et l'infiltration de la chaîne logistique par la criminalité organisée.

QUOI

Guidance DG TAXUD publiée le 14 avril 2026 — **non contraignante**

QUI

Les AEO, quel que soit le type d'autorisation, et tous les acteurs de la chaîne logistique

ENJEU

Détecter les activités suspectes, y compris la complicité interne

LE POINT CLÉ

Cette guidance **ne crée pas de nouvelle obligation juridique** : elle est explicitement présentée comme une **recommandation, non juridiquement contraignante**. Mais elle n'est pas sans effet. Elle explicite **comment les obligations AEO qui existent déjà** — contrôles internes, information de la douane, sûreté et sécurité — doivent s'appliquer aux activités suspectes liées à la criminalité. Un titulaire d'autorisation qui néglige ces obligations s'expose à une **réévaluation, une suspension ou une révocation** de son statut. La guidance annonce par ailleurs qu'elle prépare le **futur cadre légal du Code des douanes de l'Union** : ce qui est aujourd'hui recommandé a vocation à devenir obligatoire.

2. Pourquoi cette guidance ?

Les ports, aéroports et plateformes logistiques européens sont devenus des cibles privilégiées de la criminalité organisée. Le constat qui fonde la démarche est frappant : la guidance s'appuie sur le rapport de l'**Organisation mondiale des douanes** consacré à l'infiltration des chaînes logistiques maritimes, dont il ressort que des **complices internes** sont impliqués dans **68 % des cas de détection** recensés. La menace ne vient donc pas seulement de l'extérieur de l'entreprise : elle passe par ses propres collaborateurs, ses prestataires et ses accès.

La guidance s'inscrit dans un ensemble d'initiatives européennes convergentes : la **stratégie de l'UE en matière de drogue**, la **stratégie portuaire européenne**, l'**Alliance européenne des ports**, la plateforme **EM-PACT** et la **stratégie de l'Union pour la préparation**, ainsi que les principes de **partenariat public-privé** promus dans la législation douanière.

La logique affichée est **gagnant-gagnant** : l'entreprise qui coopère protège ses marchandises et sa réputation et se positionne comme un **partenaire plus fiable** ; la douane, en retour, partage son analyse du risque.

3. Qui est concerné ?

La guidance s'appuie sur le partenariat existant avec les **opérateurs économiques agréés**, mais son périmètre déclaré est plus large : elle vise les autorités douanières et les opérateurs économiques, c'est-à-dire **l'ensemble des acteurs de la chaîne d'approvisionnement intervenant dans le transport et la logistique, tous modes confondus**.

- **Tous les AEO**, quel que soit le type d'autorisation détenue — **AEOC** (simplifications douanières), **AEOS** (sûreté et sécurité) ou **AEOF** (combiné) : la guidance invite explicitement l'ensemble des titulaires à signaler, sans se limiter aux seuls AEOS.

- **Les opérateurs sans statut AEO** sont **encouragés** à suivre la même approche de partage d'informations. Pour eux, la démarche reste volontaire : elle ne s'appuie pas sur les obligations attachées à une autorisation.
- **Les infrastructures critiques** : ports, aéroports et plateformes logistiques.

En pratique : importateurs et exportateurs, transitaires et représentants en douane, transporteurs de tous modes, manutentionnaires et terminaux, entrepositaires, prestataires logistiques et acteurs du commerce électronique.

4. Les obligations qui existent déjà

C'est le cœur du raisonnement de la Commission : la coopération demandée n'est pas une nouveauté juridique, elle découle de dispositions **déjà en vigueur**. Les voici, avec ce qu'elles impliquent concrètement.

Disposition	Ce qu'elle impose
Art. 23(2) CDU	Le titulaire d'une autorisation informe la douane sans délai de tout élément survenu après la décision et susceptible d'influer sur son maintien ou son contenu .
Art. 25(1)(f) AE CDU	Une organisation administrative adaptée à la taille et à l'activité, et des contrôles internes permettant de prévenir, détecter et corriger les erreurs, ainsi que de prévenir et détecter les transactions illégales ou irrégulières .
Art. 25(1)(i) AE CDU	Les employés concernés sont instruits d'informer la douane dès qu'une difficulté de conformité est découverte, et des procédures sont établies pour cette information.
Art. 25(1)(j) AE CDU	Des mesures de sécurité appropriées protégeant le système informatique contre l'intrusion non autorisée et sécurisant la documentation de l'opérateur.
Art. 39(e) CDU Art. 28 AE CDU	Les critères de sûreté et de sécurité de l'AEOS : sécurité des bâtiments et des accès, des unités de fret, des partenaires commerciaux, du personnel et de la sensibilisation à la sécurité.
Art. 13 CDU	Le cadre général de l' échange d'informations entre les douanes et les opérateurs économiques.
Annexe 4 des lignes directrices AEO	Des exemples d'informations à partager avec la douane : incident de sécurité grave, intrusion de personnes non autorisées, interférence informatique (y compris manipulation non autorisée ou suspecte de données), cambriolage, détection d'une fraude ou d'une malveillance de partenaires commerciaux, d'employés ou de toute autre personne.
Dir. (UE) 2019/1937 RGD	La protection des lanceurs d'alerte et le respect de la protection des données encadrent les dispositifs de signalement à mettre en place.

LA CONSÉQUENCE À RETENIR

Si votre organisation détecte une activité suspecte et ne la signale pas, ce n'est pas la guidance que vous enfoncez — ce sont potentiellement l'**article 23(2) du CDU** et l'**article 25(1)(i) de l'acte d'exécution**. La guidance rappelle en outre que la douane peut engager des procédures de **réévaluation, de suspension ou de révocation** de l'autorisation, et qu'informer la douane **ne dispense pas** l'opérateur de ses autres obligations de déclaration.

5. Les signaux d'alerte à reconnaître

La guidance reconnaît qu'une liste exhaustive est impossible — « *une activité suspecte peut être toute action ou tout événement qui soulève des doutes quant à sa légitimité* ». Elle propose néanmoins une **liste d'indicateurs concrets**, dont beaucoup recoupent directement les critères de sûreté et de sécurité de l'AEOS. C'est l'outil le plus directement exploitable du document : il peut servir de base à votre grille de vigilance interne.

Catégorie	Indicateurs cités par la guidance
Sécurité des sites et des accès	Véhicules circulant sans but apparent ou stationnant à des endroits inhabituels ; personnes cherchant à entrer ou sortir en se dissimulant ; accès aux locaux non enregistrés ; clôtures ouvertes, trous dans les grillages, structures permettant l'escalade.
Reconnaissance et collecte d'informations	Personnes photographiant les infrastructures ou le personnel ; inconnus, en ligne ou sur site, s'informant sur les procédures, la sécurité ou les localisations sans justification ; personnes examinant camions, navires, conteneurs ou installations ; menaces envers le personnel.
Conteneurs, scellés et mouvements	Conteneur ouvert à un endroit inapproprié ; mouvements anormaux de conteneurs ou de moyens de transport ; changements de routage non planifiés ; anomalies ou bris de scellés ; alertes émises par des scellés électroniques ou intelligents ; embarquement de personnes non autorisées.
Personnel — le risque interne	Collaborateur effectuant des tâches étrangères à ses fonctions ; présence en dehors des horaires habituels ; changement abrupt de poste ou de tâches ; élévation soudaine du niveau de vie ; propositions faites aux employés de « gagner de l'argent » ; accès non autorisé aux systèmes informatiques ; répartition suspecte des responsabilités entre collaborateurs.
Clients et transactions	Sous-évaluation ou surévaluation de la valeur ; paiements en espèces ; décisions logistiques dépourvues de logique économique ; clients dont les données d'entreprise ne sont pas traçables ; clients ignorant les caractéristiques de leurs propres produits.

LE POINT SENSIBLE : LA MENACE INTERNE

La catégorie « personnel » est celle que les entreprises intègrent le moins spontanément dans leur dispositif de sûreté, alors que c'est celle qui pèse le plus lourd dans les statistiques. La guidance en tire une recommandation directe : prévoir un **canal de signalement interne sécurisé et permettant l'anonymat**, afin que les collaborateurs puissent alerter **sans crainte de représailles**. Ce dispositif s'articule avec la **directive (UE) 2019/1937** sur la protection des lanceurs d'alerte et doit être conçu dans le respect du **RGPD**.

6. Comment signaler : à qui, quand, quoi

À qui

Au **point de contact désigné** au sein de l'administration douanière compétente pour votre autorisation. La guidance recommande aux douanes de désigner un tel point de contact unique et de communiquer aux opérateurs les canaux à utiliser selon l'**urgence** et la nature de l'irrégularité. Son annexe 2 recense par ailleurs des **lignes de signalement (« whistleblowing lines »)** nationales — une liste **partielle**, qui ne couvre pas tous les États membres et dans laquelle la Belgique ne figure pas.

EN BELGIQUE : PORTWATCH

La Belgique figure parmi les quatre initiatives nationales documentées à l'annexe 1, avec **PortWatch** (**portwatch.be**), le point de signalement central du gouvernement fédéral — géré par le **SPF Mobilité et Transports** — pour les situations suspectes dans et autour des ports belges, **Anvers, Gand, Zeebrugge et Ostende**. Le signalement se fait **en ligne et peut être totalement anonyme** ; les données personnelles éventuellement communiquées ne sont transmises qu'aux services de police autorisés. En cas d'**urgence immédiate**, le réflexe reste l'appel au **101**.

PortWatch complète, sans les remplacer, vos obligations de notification à l'Administration générale des Douanes et Accises au titre de votre autorisation AEO.

Quand

- **Dès que possible** pour toute activité suspecte : la guidance insiste sur le caractère déterminant du **délai**, puisque c'est lui qui rend une intervention douanière encore utile.
- **Sans délai** lorsque l'élément est susceptible d'influer sur le maintien ou le contenu de l'autorisation (article 23(2) du CDU).

Quoi : le contenu de la notification

La guidance précise les informations qu'un signalement devrait comporter :

- la **description** de la transaction irrégulière, de l'activité suspecte ou de la manipulation non autorisée ;
- le **lieu, la date et l'heure** de la détection ;
- l'**identification des parties impliquées** ou, à défaut, tout élément de description des personnes ou organisations concernées ;
- les **moyens de transport** et/ou les **opérations en ligne** impliqués ;
- tout autre **détail pertinent** ou **document** utile.

À la demande de la douane, l'opérateur peut en outre partager, sur base volontaire : le **nom des prestataires de services**, l'accès à des données utiles (**horaires, plans de chargement, systèmes de suivi et de traçabilité**), les **signaux de scellés intelligents** et les **mouvements de conteneurs**, ainsi que les **images de vidéo-surveillance**.

Par quel canal

Par des **canaux sécurisés** convenus à l'avance — messagerie sécurisée ou téléphone —, l'objectif étant aussi de **protéger les collaborateurs et les sites** lorsqu'une marchandise illicite est découverte. La guidance encourage la mise à disposition d'une **option de signalement anonyme** et cite, à titre d'exemple de bonne pratique, l'existence de **systèmes d'alerte 24/7** permettant de solliciter rapidement une intervention douanière.

7. Ce que vous pouvez attendre de la douane

La guidance est explicitement **bidirectionnelle** : elle formule aussi des recommandations à l'adresse des administrations douanières. C'est un levier utile dans votre dialogue avec l'AAD&A.

- **Un point de contact désigné**, servant de guichet unique pour les signalements ; certains États membres ont mis en place, en complément, un **système d'alerte 24/7**.
- **Le partage des tendances criminelles**, des **modes opératoires** et des risques identifiés, sous une forme exploitable pour soutenir votre détection.
- **Un retour d'information** et des **analyses post-incident**, pour vous aider à comprendre les vulnérabilités exploitées.

- Une **diffusion coordonnée** des informations reçues via le **cadre commun de gestion des risques** et le **système CRMS**, dans des conditions de confidentialité et de sécurité.
- Une **approche partenariale** : encourager le signalement **sans crainte de sanction**, éviter que le signalement se traduise par des **retards opérationnels**, et conduire équitablement les éventuelles procédures de réévaluation, de suspension ou de révocation.

L'annexe 1 documente quatre modèles nationaux dont s'inspirer : la **Belgique** (PortWatch), la **Suède** (protocoles d'accord, **142 présentations à 2 500 partenaires** et 13 nouveaux protocoles signés en 2025), les **Pays-Bas** (**Strong Logistics**, la chaîne numérique fermée **Secure Chain** à Rotterdam, l'équipe pluridisciplinaire **HARC**) et la **Hongrie** (accord bilatéral écrit de partage d'informations de risque, réservé aux titulaires AEOC ou AEOF et limité à la période *postérieure à la mainlevée* des marchandises).

8. Votre plan d'action et notre accompagnement

Voici les points sur lesquels une entreprise — AEO ou non — a intérêt à se positionner dès maintenant :

- | | |
|--|---|
| ✓ Désigner un point de contact interne et son supérieur. | ✓ Revoir la sécurité IT et les droits d'accès aux systèmes. |
| ✓ Identifier le point de contact douanier et le canal d'urgence. | ✓ Renforcer la gestion des scellés et leur enregistrement. |
| ✓ Formaliser une procédure de détection et de signalement . | ✓ Vérifier et suivre vos partenaires commerciaux . |
| ✓ Donner des instructions écrites au personnel (art. 25(1)(i)). | ✓ Consigner les incidents et trancher ce qui relève de l'art. 23(2). |
| ✓ Sensibiliser et former les équipes aux signaux d'alerte. | ✓ Contrôler la conformité RGPD des dispositifs mis en place. |
| ✓ Ouvrir un canal interne sécurisé et anonyme de signalement. | ✓ Mettre à jour votre auto-évaluation AEO et vos procédures. |
| ✓ Revoir la sécurité physique : clôtures, accès, vidéosurveillance. | ✓ Anticiper la future réforme du CDU , qui rendra ce cadre contraignant. |

UN DOCUMENT VIVANT, PRÉCURSEUR DU FUTUR CDU

La Commission qualifie sa guidance de « **précurseur essentiel** » du futur cadre légal et annonce une **approche par étapes** : le document sera régulièrement actualisé pour suivre l'évolution des menaces. Les entreprises qui structurent aujourd'hui leur dispositif de détection et de signalement prendront une avance directement valorisable lors de leurs prochains audits et réévaluations AEO.

Comment Customs Conform IT vous accompagne

- **Audit AEO** au regard de la guidance : contrôles internes, procédures d'information de la douane, critères de sûreté et de sécurité.
- **Rédaction des procédures** de détection, d'escalade et de signalement, avec une grille de signaux adaptée à vos flux et à vos sites.
- **Mise à jour de votre dossier AEO** : auto-évaluation, documentation, registre des incidents et notifications au titre de l'article 23(2).
- **Formation** de vos équipes opérationnelles, administratives et de sécurité.
- **Sûreté de la chaîne et volet IT** : accès, vidéosurveillance, scellés, droits dans vos systèmes, sécurité informatique.
- **Canal de signalement interne** conforme à la directive (UE) 2019/1937 et au RGPD.

- **Préparation aux contrôles**, réévaluations et audits douaniers, et anticipation de la réforme du CDU.

9. Modèle de fiche de signalement

Un signalement n'est exploitable que s'il est **complet du premier coup**. Cette fiche reprend les informations attendues par la guidance et peut être intégrée telle quelle à votre procédure interne.

Rubrique	À compléter
Date et heure de la détection	
Lieu précis (site, quai, entrepôt, portail)	
Nature du fait constaté — transaction irrégulière, activité suspecte, manipulation non autorisée	
Personnes ou organisations concernées — identité si connue, à défaut description	
Moyens de transport ou opérations en ligne concernés — plaque, navire, n° de conteneur, n° de scellé	
Documents et preuves joints — photos, vidéosurveillance, track & trace	
Constaté par / signalement anonyme ?	
Signalé à (douane, PortWatch, police) — canal utilisé	
Date et heure du signalement	
Notification art. 23(2) CDU requise ? / suite donnée	

En cas de danger immédiat pour les personnes, l'appel au **101** précède toute formalité ; la fiche documente alors le fait *a posteriori*.

PASSONS À L'ACTION

Que vous soyez déjà titulaire d'une autorisation AEO ou que vous envisagiez de la demander, la question à trancher est simple : **si un de vos collaborateurs détectait demain une activité suspecte, saurait-il quoi faire, qui prévenir et dans quel délai ?** Contactez **Customs Conform IT** pour un diagnostic de votre dispositif et la mise en place des procédures correspondantes.



Sources : Commission européenne, DG TAXUD, communiqué du 14 avril 2026 et « AEO — Customs Cooperation to Detect, Report and React to Suspicious Activities — Guidance document », Bruxelles, 31 mars 2026, réf. TAXUD/A3/002/2026 (annexes 1 et 2) ; Règlement (UE) n° 952/2013 (CDU), art. 13, 23(2), 39(e) ; Règlement d'exécution (UE) 2015/2447, art. 25(1) et 28 ; lignes directrices AEO, annexe 4 ; OMD, « *Infiltration of Maritime Cargo Supply Chains* » (2025) ; Directive (UE) 2019/1937 ; RGPD ; portwatch.be (SPF Mobilité et Transports).

Avertissement : cette note est une synthèse d'information générale, à jour d'août 2026, et ne constitue pas un conseil juridique. La guidance de la Commission est un document non contraignant, appelé à être actualisé ; les modalités pratiques de signalement doivent être confirmées auprès de l'Administration générale des Douanes et Accises et, le cas échéant, des autorités compétentes de votre secteur. © Customs Conform IT — customs-conformit.be