EUROPEAN COMMISSION
DIRECTORATE-GENERAL
TAXATION AND CUSTOMS UNION
Customs
Risk Management and Security

Brussels, 31 March 2026
TAXUD/A3/002/2026

AEO – CUSTOMS COOPERATION TO DETECT, REPORT AND REACT TO SUSPICIOUS ACTIVITIES

GUIDANCE DOCUMENT

Table of contents

1. Introduction

The purpose of this document is to enhance the capabilities of customs authorities and economic operators, i.e. all supply chain actors involved in transport and logistics in all modes of traffic to identify, follow up, and prevent irregularities, including those related to security and safety threats, such as drug trafficking, and to organised crime, as well as to other forms of illicit activity.

This will be achieved by fostering enhanced two-way cooperation between customs authorities and economic operators, in line with the EU Drugs, the EU Ports Strategy and principles of public private partnership to secure goods supply chains enshrined in the EU customs legislation. The cooperation consists of:

- Gathering information from economic operators for customs to leverage their expertise and resources to detect and prevent irregularities

- Devising ways for custom authorities to share relevant information and knowledge in accordance with national legislations to enhance economic operators' capacity to detect fraudulent shipments and suspicious parties.

The present initiative is building on the existing cooperation between Authorised Economic Operators (AEOs) and customs authorities, aiming to deepen the level of collaboration and information sharing, enabling customs authorities to better target and prevent illicit activities. Nevertheless, all economic operators are encouraged to follow the same approach of information sharing to ultimately contribute to a safer, more secure, and more compliant trade environment.

Within the framework of the new UCC, the primary intention is to further elaborate the legal framework of the exchange of information between customs and economic operators. In the interim, following a step-by-step approach, this guidance aims to pave the way for the impending legal setting. By fostering a transparent and collaborative environment, this endeavour seeks to establish a robust foundation for the forthcoming regulatory framework. As the new UCC takes shape, this guidance will serve as a vital precursor, promoting a culture of cooperation and compliance amongst stakeholders.

This guidance is a recommendation; it is not legally binding and serves an explanatory purpose. It does not attempt to address every possible scenario. Instead, it focuses on areas where challenges are most frequently encountered.

2. Threats and response to threats

2.1. Abuse of legitimate trade is extensive and growing

The European Union faces a multitude of threats to its security and stability, including the pervasive influence of organised crime using illicit trafficking of goods as income source, such as the proliferation of illicit weapons or the smuggling of drugs. These threats not only compromise the safety of EU citizens but also undermine the economic and social fabric of the societies. Customs authorities play a vital role in combating these menaces, acting as the frontline guardians against such illegal activities.

Organised crime groups use sophisticated methods to evade detection[1], necessitating customs authorities to employ advanced technologies and collaborate more not only with customs and other authorities, but also with economic operators. The role of customs in preventing these threats is multifaceted, involving not just the physical inspection of goods but also intelligence gathering, risk assessments, and the use of technology like scanning equipment and data analytics to identify and intercept illegal shipments. The success of these efforts is crucial to the security and prosperity of the EU.

Organised crime poses a multi-dimensional threat to security, economy, rule of law, public safety, and social trust. Additionally, it also leads to significant financial losses. The European Public Prosecutor's Office in its Annual Report 2023 estimates that damage to the EU budget from serious, cross-border VAT fraud alone was €11.5 billion. According to Eurojust's Annual Report 2023[2], organised crime profit from illicit activities in the EU is estimated at €139 billion per year and it states that more than 80% of EU criminal networks use legal business entities to hide or launder crime proceeds[3], meaning that maintaining integrity of AEOs is getting even more crucial.

To effectively safeguard the European Union against the myriad of threats posed by illicit activities, it is imperative to recognise the critical role of customs as the first line of defence at the border. However, it is also acknowledged that economic operators, as primary stakeholders in the movement of goods, possess valuable first-hand information regarding the goods entering and leaving the Customs Union. Enforcement is rather challenging and requires enormous resources. In 2024, under the EU's EMPACT (European Multidisciplinary Platform Against Criminal Threats) initiative, 6 635 investigations were performed. Furthermore, there were 13 575 arrests and seizures of €1,05 billion in assets / money and more than 85 tons of drugs[4]. The latest EU's Serious and Organised Crime Threat Assessment (SOCTA) identifies as key threat from organised crime migrant smuggling, drug trafficking, firearms trafficking, "waste crime" but also digital threats such as cyber-attacks and ransomware.

1. [1] See for example Europol report: evolving tactics in maritime cocaine trafficking operations - Innovative concealment methods and diversified routes highlight the need for enhanced international cooperation | Europol
[2] Organised crime: Council reports on EU-wide crime-fighting actions - Consilium
[3] Organised crime: Council reports on EU-wide crime-fighting actions - Consilium
[4] 2025_2020_empact-factsheets-2024_02.pdf

2.2. Enhancing the collective response to a common threat

While several Member States have implemented their own initiatives to address the evolving threats (Annex 1), including enhanced cooperation between customs authorities and other relevant authorities such as other law enforcement, port and aviation authorities, as well as contractual arrangements or voluntary schemes with economic operators to share information with customs about irregularities, these efforts are valuable but insufficient on their own. The nature of these threats is inherently transnational, and therefore, a more coordinated and comprehensive response at the EU level is necessary to effectively counter them.

With the future Customs reform, the European Ports Alliance, the EU Ports Strategy, and initiatives under the Preparedness Union strategy, the EU and its Member States are taking steps to enhance the security of supply chains, means of transport, and critical infrastructure such as harbours, airports and logistical hubs, notably by improving risk analysis, facilitating the cooperation and sharing of information with other agencies and authorities, and bringing collaboration with the private sector to the next level. At international level, the World Customs Organisation (WCO) is also promoting cooperation and information sharing to address the global threat of organised crime. [5]Initiatives like the Supply Chain Integrity Project aim to strengthen international cooperation and provide a framework for customs authorities and economic operators to work together, ultimately promoting a safer and more secure global trading environment. The WCO report on Infiltration of maritime cargo supply chains[6] highlights the need for cooperation between customs authorities and economic operators to prevent organised crime in maritime cargo supply chains.

In order to optimise the fight against threats, it is essential to facilitate a two-way sharing of information between economic operators and customs authorities. This collaborative approach would enable customs to leverage the knowledge and insights of economic operators to better identify and mitigate potential risks, thereby enhancing the overall security and integrity of the EU.

To benefit from this collaborative approach, economic operators are encouraged to share information related to organised crime with customs authorities. By doing so, they can secure their supply chain and better prevent the infiltration of harmful mechanisms of insecurity and corruption. Furthermore, they cannot only enhance their own security but also be perceived as an even safer and more reliable business partner, ultimately strengthening their reputation and relationships with other stakeholders.

In line with the WCO Guideline on Customs Responses to Industry Referral[7] and in accordance with the Member State's laws and regulations, customs authorities should devise ways to

---

[6] wco-report_infiltration-of-maritime-cargo-supply-chains_june-2025.pdf

[7] https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/tools-and-instruments/giis/ec0863eae1.pdf?db=web

establish a two-way flow of information with trusted traders and help them to enhance their own complementary detection capacities.

To this end, it is recommended to strengthen the information sharing, which would allow economic operators to report any suspicious activities, such as unauthorised handling of goods, suspicious movements, and other illicit activities or anomalies to customs authorities in a timely and efficient manner.

To achieve this, Member States can adopt a phased approach to intensify information exchange, commencing with initial steps such as signing Memoranda of Understanding (MoU) with trusted traders, further develop secured communication channels, and establishing clear protocols for data sharing. When implementing these measures, it is essential to take into account the relevant legal settings, including the General Data Protection Regulation (GDPR) rules, to ensure that all information exchange activities are conducted in a lawful and secure manner, thereby fostering trust and cooperation between customs authorities and the private sector.

By fostering the cooperation and information sharing between economic operators and customs and other authorities, the European Union can strengthen its defences against illicit activities, promote a safer and more secure trade environment, and ultimately protect the interests of its citizens and businesses. This approach aligns with the principles of a risk-based approach to customs control, which emphasizes the importance of collaboration and information sharing in identifying and mitigating potential risks.

A logical step in achieving this goal is to build on the existing Authorised Economic Operator (AEO) programme, which has already established a foundation for cooperation and trust between customs authorities and economic operators. The AEO programme has demonstrated the value of mutually beneficial relationships, with AEO-authorised companies already enjoying streamlined customs procedures and reduced administrative burdens. By leveraging this existing framework, we can extend and deepen the level of cooperation and information sharing.

As AEO-authorised companies already have well-established communication channels with customs authorities, we can utilize these existing relationships to facilitate the sharing of information on suspicious activities, unauthorized handling of goods, and other potential risks.

3. Existing AEO obligations

In addition to the general possibility of information exchange between customs authorities and economic operators, stipulated in Article 13 of the Union Customs Code (UCC[8]), AEOs are already subject to specific obligations, as outlined in the UCC and the AEO Guidelines[9], to

[8] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code

[9] TAXUD/B2/047/2011 – rev. 6

prevent and detect irregularities and to inform customs authorities of any compliance difficulties or factors that may impact the continuation or content of their authorisation.

- Article 25 (1) (f) Union Customs Code Implementing Act (UCC IA)[10] says that *the applicant has an administrative organisation which corresponds to the type and size of business and which is suitable for the management of the flow of goods, and has internal controls capable of preventing, detecting and correcting errors and of* ***preventing and detecting illegal or irregular transactions;***
- Article 25 (1) (i) UCC IA requires that *"the applicant ensures that relevant employees are instructed to inform the customs authorities whenever* ***compliance difficulties*** *are discovered and establishes procedures for informing the customs authorities of such difficulties*".

  The applicant should have procedures in place for notifying customs in case of customs compliance difficulties and also an appointed contact person responsible for notifying the customs authorities. Formal instructions should be addressed to employees involved in the supply chain in order to prevent possible difficulties to comply with customs requirements. All identified difficulties should be reported to the appointed responsible person (s) and/or his or her replacement(s).

- Article 25 (1) j) UCC IA stipulates that *the applicant has appropriate security measures in place to protect the applicant's computer system from unauthorised intrusion and to secure the applicant's documentation*;
- In application of Article 23 (2) UCC, "*the holder of the decision shall inform the customs authorities without delay of any* ***factor*** *arising after the decision was taken, which* ***may influence its continuation or content***".

Annex 4 of the AEO Guidelines gives some examples of information to be shared with customs authorities. The annex is not a comprehensive check list, but an indicative tool to help operators in their relationship with customs authorities for the management of their AEO authorisation(s). If the economic operator considers a fact not listed that may have an impact on its AEO authorisation, customs is to be informed. However, informing the competent customs authorities does not relieve the economic operator from other reporting duties.

Some elements of the list can be considered as suspicious activity, e.g. any serious security incident, intrusion of unauthorised persons, cyber interference, including unauthorised or suspicious manipulation with the data contained in the system of the economic operator, burglary, detection of fraud or malpractice/misconduct from business partners and/or employees and any other person.

[10] Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code

4. Cooperation - Raising awareness – A win-win situation

Cooperation is highly beneficial for all parties. Not only customs authorities gain better overview of the operations and the security measures of the economic operators, but it also helps the economic operators to better understand the possible security challenges related to their operations enabling them to optimise their processes, internal control and security measures. Optimised processes possibly result in smoother and a more efficient flow of goods, quicker passage through the terminals, increased traffic and consequently a significant boost to the business.

This collaboration also leads to improvements in internal security measures, such as the installation of enhanced CCTV systems, which can help detect and prevent irregular activities and damages on premises, ultimately resulting in significant economic benefits for the operator. Additionally, cooperation with customs enhances the security of the employees, of the premises and the business as a whole. A major benefit for the economic operator, is also to have improved implemented measures to prevent incidents that can seriously damage the reputation of the company.

By sharing information with customs authorities, they can enhance targeted risk management, facilitating prompt responses to incidents and improving the prevention of future occurrences.

Customs authorities are encouraged to share with trusted traders relevant information and knowledge, such as current criminal trends, modus operandi and risks, and where possible and permitted by legislation (including on data protection and cyber security), other actionable information to support these traders in concrete detection activities.

By sharing this information, industry can be better prepared to identify emerging and existing threats, thereby increasing the resilience of the industry and the quality and frequency of its referrals to the authorities. This information flow could also include post-incident analyses and conclusions arising from them.

Pending operational sensitivities, customs authorities might provide feedback and share post-incident analysis supporting companies' understanding of vulnerabilities that have been exploited by criminals, helping to ensure these gaps are closed in the future.

Customs authorities are encouraged to delve deeper into the potential benefits of information sharing with economic operators by adopting a step-by-step approach. One notable example of best practice is the Hungarian model (Annex 1), which is considered as a good first step to systematically integrating information sharing into the processes enhancing efficiency and transparency.

Sweden also provides another example (Annex 1) of fructuous collaboration between customs authorities and key economic operators consisting in a two-layer approach.

In summary, collaborating with customs contributes to a safer society and benefits everyone by boosting economic growth, improving security, and increasing efficiency for all parties involved; a true win-win scenario.

It is essential that customs authorities, already in the audit phase and also after granting the authorisation, raise awareness among AEOS, and in a wider sense to all economic operators which play a role in securing supply chains, about the importance and the benefits of information sharing related to suspicious activities.

Offering specific meetings, events and seminars, possibly in collaboration with other competent authorities, such as (other) law enforcement authorities is considered as a best practise to promote awareness and encourage participation.

Increasing awareness of publicly available information, such as the recently published Global Organised Crime Index for 2025[11] (a report accompanied by its updated interactive world map, offering insights into various forms of crime), as well as threat and risk analyses of EU agencies[12] and international bodies[13] as well as from national authorities, assists economic operators in improving their compliance and strengthening the security of their business partnerships.

In addition, various tools could be developed, including posters, flyers, presentations, social media or other online outreaches highlighting the importance of collaboration and information sharing.

5. Suspicious activity: the trigger for information sharing

Suspicious activities could be any action or occurrence that raises suspicions about their legitimacy. These anomalies might only be detected by the economic operators who are familiar with the usual methods and procedures, and who might identify deviations from the norm based on their experience and knowledge of the logistics flow. As they are best placed to recognise unusual patterns or events, it is essential that they alert the customs authorities, when they suspect something is amiss. However, as criminal organisations continually adapt and evolve their tactics, it is not feasible to create an exhaustive list of suspicious activities. Instead, providing some typical examples of suspicious behaviours or indicators can serve as a useful

[11] https://globalinitiative.net/wp-content/uploads/2025/10/OCINDEX_2025_DIGITAL_REPORT.pdf ; https://ocindex.net/

[12] EU Serious and Organised Crime Threat Assessment (SOCTA) 2025 in particular chapters 2 and 3: The changing DNA of serious and organised crime - EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA) | Europol; EU Drugs Report 2025 in particular on the drug situation and the drug supply, production and precursors: European Drug Report 2025: Trends and Developments | The European Union Drugs Agency (EUDA); The EU Internet Organised Crime Threat Assessment (IOCTA) 2025: Steal-deal-repeat-IOCTA_2025.pdf; The Security Advisories and Threat Intelligence of CERT-EU: CERT-EU - Publications - Security Advisories.

[13] The World Drugs Report of The United Nations Office on Drugs and Crime in particular on the drugs markets, patterns and trends: World Drug Report 2025

starting point, while also acknowledging that economic operators must remain vigilant and use their expertise to identify potential threats as they arise.

Although many of the elements on the list are closely tied to the security and safety criteria relevant to AEOS (Article 39(e) UCC and Article 28 UCC IA), it is encouraged that all types of AEOs regardless of their specific authorisation, and other economic operators follow the same lines and report any suspicious activities they may encounter. This means that even if a particular AEO is not necessarily bound by the same security and safety requirements, they are still invited to adopt a proactive approach to reporting suspicious activities, thereby contributing to a more secure and compliant supply chain.

Examples of suspicious activities

- Vehicles turning aimlessly or stopping in unusual places
- Unauthorised persons boarding a vehicle or boat
- People or vehicles trying to enter or leave the premises with someone else
- People or vehicles entering the premises without registration
- People taking photographs of the premises' infrastructure or persons on the premises
- Open gates, fences with holes in them or structures to facilitate climbing
- People examining trucks, ships, containers or facilities
- An (open) container in the wrong or unusual place
- Unknown persons on site requesting specific information (operating procedure, security, specific location, etc.) for no apparent or valid reason
- Seal anomalies, or broken seals found, alerts of intrusion or unusual movements of containers in the case of electronic / smart seals or means of transport within the perimeters of logistics hubs (ports, warehouses) or outside those areas (un-planned change of routing)
- Unknown persons online requesting specific information (operating procedure, security, specific location of goods movement, etc.) for no apparent or valid reason
- Staff members performing activities outside of their ordinary duties
- Illogical logistics decisions or planning
- Suspicious transactions (under- or over valuation, cash payments, etc)
- Illogical distribution of duties among employees or shifts
- A new customer from whom (almost) no company data is traceable
- Customers who know almost nothing about the products they want to import
- A member of staff who suddenly has a very high standard of living for no reason
- Offers to "earn some money" made to staff working at the premises
- Staff members who are suddenly in or around the premises outside their working hours
- Someone wanting to abuse position, remit or knowledge within the premises and threatening someone working on the premises
- Non-authorised access to IT systems

In addition to the existing AEO reporting obligations, AEOs and other economic operators are encouraged to notify the customs authorities as soon as possible in case of suspicious activities, sharing as much information as possible.

The notification preferably includes:

- The description of the irregular transaction, suspicious activity or unauthorised handling of goods
- The place, date and time of detection
- The identification of the parties involved if possible or as much as possible information to help identify those parties (description of persons, organisations involved etc.)
- Means of transport (e.g. vehicles, containers, vessels, aircrafts) and/or online operations involved
- Any other relevant details or supporting documentation.

In the frame of the cooperation with customs authorities, AEOs can further enhance the effectiveness of the information-sharing process by making additional commitments. For instance, on a voluntary basis and upon request by customs, they can share further (sensitive) information such as the names of service providers, and provide access to relevant data, including schedules, traffic and loading plans, tracking and tracing systems, smart seal signals and movements of containers and means of transport, and video surveillance systems that monitor the premises where goods are loaded, unloaded, transhipped, or handled. By sharing more information, AEOs can provide customs authorities with a more comprehensive understanding of their logistics operations, enabling them to better identify potential security risks and take proactive measures to prevent them. This increased level of transparency and cooperation can lead to better outcomes, including improved security, reduced risks, and more efficient customs procedures.

It is also crucial that information is shared in a timely manner, as soon as possible, to ensure that customs, (other) law enforcement and competent authorities can take prompt action to address potential threats. Therefore, AEOs are encouraged to report suspicious activities as quickly as possible, using the designated secure methods to facilitate swift and effective actions.

Each national customs authority is best placed to determine the most effective **procedures for receiving, transferring and handling information** from and to economic operators. To facilitate sharing of information, it is recommended that customs authorities designate a specific contact point within their administration that can serve as a single point of contact for operators to report suspicious activities. The customs authority responsible for the AEO authorisation should inform AEOs about the designated contact point and/or the alternative channels depending on the urgency and nature of the possible irregularities. For instance, a **24/7 alert system is** enabling economic operators to quickly request customs intervention, thereby ensuring a rapid response to potential security threats.

To guarantee the secure transmission of sensitive information, it is recommended to establish accepted methods, such as secure email or phone calls. This approach also helps to safeguard employees and secure premises in the event of discovering drug or other illicit products or identifying potential risks.

The WCO report on "Infiltration of Maritime Cargo Supply Chains" highlights the significant risk of internal conspirators, with a staggering 68% involvement in detection events, emphasising the need for robust security measures. This high risk, which is possibly present in relation to all means of transport, has a direct link to the AEO personnel security criteria as internal conspirators often exploit vulnerabilities within the supply chain. Against this background, it is advisable to provide the option for reporting suspicious activities also anonymously (whistleblowing), as many Member States already offer, for example, through a dedicated hotline or online form. This anonymity can help encourage operators to come forward with information, without fear of reprisal or repercussions, thereby enhancing the overall effectiveness of the information-sharing process.

The EU Whistleblower Protection Directive[14] (Directive) aims to establish a framework for the protection of persons who report breaches of EU law, providing a safe and confidential channel for whistleblowers to share information.

Establishing **internal whistleblowing systems** within the company is regarded as a best practice in preventing supply chain infiltration, as it provides a secure and confidential mechanism for employees to report concerns or suspicions about potential wrongdoing, allowing for early identification and mitigation of risks.

Additionally, **external whistleblowing mechanisms** are also important, as they can provide an alternative channel for reporting suspicious activities, in particular when uncertainty is present on the foothold of internal conspirators within a company, further enhancing the security and integrity of supply chains.

Pursuant to the Directive, several Member States have established national whistleblower reporting lines, which can complement the security measures implemented by the AEOs, as outlined in Annex 2.

Last, but not least, it has to be emphasized that to effectively address threats across the entire supply chain and external borders, the shared information must not stay at the local, regional, or national customs authorities' levels. Instead, relevant information shall be shared timely with all customs authorities in the frame of the Common Risk Management Framework utilising CRMS (Customs Risk Management System), and for this purpose designated contact points, ensure comprehensive coverage, coordination, and secure, trusted and confidential handling of relevant information.

[14] Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law

6. Management of the AEO authorisation – continuous cooperation

To promote a collaborative approach, enhancing the internal control mechanisms of AEOs can significantly improve both compliance and the effective monitoring of AEO status by authorisation holders. When legal obligations, particularly those involving information sharing and internal controls, are effectively met, the benefits of cooperation are evident. Customs authorities, guided by legislation and Commission guidelines play a crucial role in the management of the AEO authorisations, performing reassessment, suspension, or revocation processes.

However, these measures are strengthened through cooperative efforts, and economic operators should be encouraged to identify and refer suspicious activities without fear of punishment or unnecessary delays to their operations as a result of their referral. Customs needs to work with economic operators as partners in this process.

A key aspect of cooperation is the emphasis on maintaining robust internal controls as stipulated in Article 25(1)(f) of the UCC IA, ensuring that economic operators have the necessary systems in place. By establishing procedures and training employees to inform customs authorities of any potential compliance difficulties, as per Article 25(1)(i) of the UCC IA, and by additional voluntary information sharing economic operators contribute to a smoother operation and mitigation of risks.

Customs authorities should collaboratively assess the adequacy of an operator's internal controls to efficiently identify illegal or irregular transactions, thereby enforcing regulations in partnership rather than in isolation. Through joint efforts, both authorities and AEOs can work towards sustainable compliance and the integrity of the authorisation status, fostering a proactive rather than reactive environment within the international trade framework.

7. Collaborative efforts – a dynamic approach

To maintain a robust and effective collaboration and regular update of this guidance that responds to the constantly changing modusoperandi of illicit actors, it is crucial that the partnership between customs authorities and economic operators remains dynamic, agile, and adaptive. It should provide a framework of cooperation where both parties stay informed about emerging threats and respond swiftly. This demands a deeper and more operational level of cooperation, one that delves into the sensitive aspects of joint threat assessment and mitigation. To achieve this, ongoing dialogue and collaboration are essential, with all stakeholders working together to continuously update and refine this guidance, effectively making it a living document that evolves to address new challenges and stay ahead of emerging risks.

8. **Annex 1: National customs initiatives to report suspicious activities and to share information with economic operators**

Belgium - PortWatch.be

The PortWatch initiative in Belgium is an essential tool in combating organised crime in Belgian seaports. It allows anonymous reporting of suspicious activities in Belgian ports, including Antwerp, Ghent, Zeebrugge, and Ostend. Its objective is to enhance port security by encouraging port workers, waterway users, fishermen, and office employees to report any unusual situation. Reports can be made via the **PortWatch.be** website (available in 5 languages DE, EN, FR, NL and SP) where users can describe the situation provide details about suspects and even add photos or videos. The confidentiality of information is strictly respected to ensure the safety of people who report suspicious activities.

This initiative is supported by the Minister of the North Sea, DG Navigation of FPS Mobility and Transport and Federal Police. It also aims to create a safer port environment by facilitating cooperation between different actors in the maritime sector. As part of this initiative, Customs is involved by:

- Working closely with police to assess reports received via PortWatch. These reports may include suspicious activities related to smuggling, drug trafficking, and other forms of crime.
- Analysing information provided by anonymous reports. This helps better understand threats to ports and take targeted measures to counter them.
- Collaborating with other services to inspect ships and verify compliance with regulations.

Hungary

The national Customs Act related to Article 13 of UCC states that in order to support the self-monitoring of an economic operator, the customs authority may communicate risk information referred to in Article 5 (7) of UCC to the economic operator, but only if he/she is a holder of an AEOC or an AEOF authorisation, and only after the release of the goods. The risk information may only relate to the customs declaration or re-export declaration in respect of which the holder of AEOC or AEOF authorisation concerned has acted in his/her own name and on his/her own behalf.

This practice can only operate on the basis of a bilateral (written) agreement between the head of the Customs Administration and the holder of the AEOC or AEOF authorisation and it reduces the administrative burden and costs of both parties. The provision, in addition to serving the EU and national financial interests, broadens the scope of national benefits granted to AEOs

and also strengthens cooperation between the customs authority and AEOs. The provision does not restrict the customs authority from introducing post-release controls in relation to the declaration concerned, if justified.

The Netherlands - Strong Logistics & Secure Chain Programme

The Netherlands has started the so-called "Strong Logistics" programme. The NL project group TFOC (Transport Facilitated Organised Crime) from the National Police Unit started this programme 5 years ago in 2020 in order to prevent criminal activities in the international supply chain, mainly focussing on transport companies (in the NL about 25.000 companies). Main aim is to visit those transport companies and create awareness, talking to truckdrivers, planners and management about ways to prevent illegal and criminal activities in order to combat and dismantle criminal organisations.

Starting this project group was initiated by the NL under an EMPACT (European Multidisciplinary Platform Against Criminal Threats) action. NL customs officers are also participating in this project group consisting of several enforcement agencies. During these last 5 years, the United Kingdom, Ireland, Denmark, Sweden, Norway and Finland joined the initiative. In all these countries similar project groups have started and combined international actions and periodical meetings are planned.

In the Port of Rotterdam a « Secure Chain Programme « has been implemented by law enforcement authorities, port authority and private companies (deepsea shipping lines, terminals and cargodoors). In this programme a closed digital logistic secure supply chain has been created by trusted parties processing import containers from non-EU countries. Only trusted parties are allowed to share « need to know » information via a secure Port Community System, which further strengthen digital security and optimizes port logistics.

Rotterdam Seaport Police also share information with public operators through the HARC-document. This document includes general (risk) information about criminal trends and important (drug) seizures and it is shared with public operators by the specialised Hit and Run Cargo (HARC) team. The team, which includes 4 main partners (NL Customs-expert team-, Seaport Police, Fiscal Intelligence unit (FIOD) and Prosecutor's Office Rotterdam), has been operational for 25 years and mainly focuses on combatting serious crime related to drugs trafficking via Rotterdam seaport and Amsterdam airport.

Sweden

The Cooperation against Customs-Related-Crime programme establishes a frame to combat infiltration in the economic operators and its flows to combat smuggling and customs-related crime. It encourages companies' employees to contact Swedish Customs on their own initiative and, via a Memorandum of Understanding, creates and maintains contact channels.

Swedish customs made 142 presentations for 2500 “partners” in 2025 on how organised crime uses legal companies for smuggling in commercial consignments and signed 13 new MoU agreements.

These trainings on modus operandi with tips on what can raise doubts give economic operators the capacity to detect suspicious transactions at the very early stages of the supply chain, thus even before any information or data is available to the customs.

Through the signature of an MoU, customs and the economic operator can frame their collaboration and more systematic information sharing and organise follow-up of suspicious consignments.

9. **Annex 2 Member States whistleblowing lines**

Austria

e-mail: cpc@bmf.gv.at

Tel : +43 50 233 569058

Republic of Cyprus

e-mail: cmichael@customs.mof.gov.cy, lpanaou@customs.mof.gov.cy

Tel.: +357 22601698, +357 22601668

Republic of Croatia

Customs: https://carina.gov.hr/istaknute-teme/stop-korupciji/2385; Tel: +385 0 800 12 22; e-mail: prijava.korupcije@carina.hr

Police: Tel: +385 0 800 50 92; e - mail: korupcija@mup.hr

Office for the Suppression of Corruption and Organised Crime (USKOK):

Tel: +385 1 4591 874; E – mail: uskok.zg@uskok.hr

Czech Republic

https://celnisprava.gov.cz/cz/o-nas/kontakty/Stranky/oznameni-porusovani-predpisu.aspx

https://celnisprava.gov.cz/cz/o-nas/spolecne-proti-korupci/Stranky/default.aspx -

Denmark

https://politi.dk/om-politiet/kontakt-politiet/tip-politiet

https://whistleblower.dk/

Estonia

EN:https://www.emta.ee/en/business-client/board-news-and-contact/contacts/fraud-hotline

EE : https://www.emta.ee/ariklient/amet-uudised-ja-kontakt/kontaktid/vihje-andmine

Tel: +372 800 4444 (24/7) e-mail: **vihje@emta.ee**

Finland

https://vihjeet.tulli.fi/?lang=en for non-urgent cases

Tel: 24/7: +358 (0)800 1 4600 for urgent cases

France

e-mail: ids@douane.finances.gouv.fr .

Germany

Ports of Bremerhaven: www.bkms-system.com/tatort-hafen; +49 421 5154 7000

Port of Hamburg: https://www.bkms-system.com/bkwebanon/report/clientInfo?cin=D83tg7&c=-1&language=eng

Greece

https://www.aade.gr/sites/default/files/kataggelies/

Hungary

HU : https://nav.gov.hu/ugyfeliranytu/keressen_minket/kozerdeku_bejelentes_panasz

EN : https://nav.gov.hu/en/contact/public-interest-disclosure-complaint

Ireland

Tel: 1800 295 295 - Customs Drug Watch Confidential Freefone

Email: NPC@revenue.ie.

Lithuania

https://muitine.lrv.lt/lt/Praneskite-apie-pazeidima-arba-nusikaltima/

Tel: +370 800 555 44

E-mail: pasitikek@lrmuitine.lt

The Netherlands

NL (police): www.meldmisdaadanoniem.nl Tel : +31(0) 800-7000 (anonymous)

NL Customs Contact Centre Tel:: +31(0)800-0143

NL Customs Excise fraude: E-mail: douanemeldpuntaccijns@douane.nl

Portugal

https://info.portaldasfinancas.gov.pt/pt/at/Canal_de_Denuncia/Paginas/default.aspx

Slovak Republic

Kriminálny úrad f... - PFS

Tel. +421 (800) 110110,

email: oskufs@financnasprava.sk

Slovenia

Tel.: 080 11 22

e-mail: gfu.fu@gov.si

Sweden

SE:https://www.tullverket.se/foretag/internationellhandel/samradochsamverkan/samverkanmottullbrottslighetsmt.4.792224361590183a4d3b92.html

EN:https://www.tullverket.se/en/startpage/business/applyanddeclare/authorisationsandregistrations/aeoauthorisedeconomicoperator/cooperationagainstcustomsrelatedcrimes.4.7df61c5915510cfe9e76543.html

https://www.tullverket.se/en/startpage/contactus/contact/contactus/reportacrimetoswedishcustoms.4.1595e959179a7cfd5c7693.html